HOTWIRE™ DSLAM FOR 8310 MVL™ AND 8510 RADSL CARDS

USER'S GUIDE

Document No. 8000-A2-GB26-10

January 1999

PARADYNE™

Notice

Warranty, Sales, and Service Information

Contact your local sales representative, service representative, or distributor directly for any help needed. For additional information concerning warranty, sales, service, repair, installation, documentation, training, distributor locations, or Paradyne worldwide office locations, use one of the following methods:

- **Via the Internet:** Visit the Paradyne World Wide Web site at http://www.paradyne.com
- **Via Telephone:** Call our automated call system to receive current information via fax or to speak with a company representative.
  - — Within the U.S.A., call 1-800-870-2221
  - — Outside the U.S.A., call 1-727-530-2340

Trademarks

Patent Notification

Hotwire MVL products are protected by U.S. Patents: 4,637,035, 4,744,092, 4,669,090, 5,291,521 and 5,280,503. Other U.S. and foreign patents pending.

Document Feedback

We welcome your comments and suggestions about this document. Please mail them to Technical Publications, Paradyne Corporation, 8545 126th Ave. N., Largo, FL 33773, or send e-mail to userdoc@eng.paradyne.com. Include the number and title of this document in your correspondence. Please include your name and phone number if you are willing to provide additional clarification.

Printed on recycled paper

Contents

5 Monitoring the Hotwire DSLAM

6 Diagnostics and Troubleshooting

A Download Code

B Traps

Glossary

Index

About This Guide

Document Purpose and Intended Audience

This guide describes how to configure and operate the software component of the Hotwire Digital Subscriber Line Access Multiplexer (DSLAM) system. It is intended for administrators and operators who maintain the networks that support Hotwire operation.

A basic understanding of internetworking protocols and their features is assumed. Specifically, you should have familiarity with Simple Network Management Protocol (SNMP), Network Management Systems (NMSs), and the following internetworking concepts:

- TCP/IP applications
- IP and subnet addressing
- IP forwarding (also referred to as IP routing)
- Bridging

It is also assumed that you have already installed either the Hotwire 8600, 8800, or 8810 DSLAM. If you have not done so already, refer to the appropriate Hotwire DSLAM Installation Guide for installation instructions.

NOTE:

It is highly recommended that you read the *Hotwire DSLAM for 8310 MVL and 8510 RADSL Cards Network Configuration Guide* before you begin to use this guide and the Hotwire software. The *Hotwire DSLAM 8310 MVL and 8510 RADSL Cards Network Configuration Guide* provides introductory information about the Hotwire DSLAM network models and theories.

Document Summary

Section	Description
Chapter 1	*Hotwire DSLAM System Description.* Provides an overview of the Hotwire 8600 and 8800 systems.
Chapter 2	*Hotwire Menus and Screens.* Describes the operation of Hotwire menus, screens, and commonly used navigation keys. Also provides instructions on how to log in and log out of the system.
Chapter 3	*Configuring the Hotwire DSLAM.* Describes the required procedures for configuring the Hotwire system.
Chapter 4	*8310 MVL and 8510 RADSL Card Configuration.* Describes the optional procedures for configuring the DSL cards on the Hotwire system.
Chapter 5	*Monitoring the Hotwire DSLAM.* Describes operator programs that monitor the Hotwire system.
Chapter 6	*Diagnostics and Troubleshooting.* Describes common Hotwire operational problems and solutions.
Appendix A	*Download Code.* Describes how to work with the Download Code and Apply Download menus.
Appendix B	*Traps.* Describes the traps that are generated by the Hotwire system.
Glossary	Defines acronyms and terms used in this document.
Index	Lists key terms, acronyms, concepts, and sections in alphabetical order.

Product-Related Documents

Document Number	Document Title
5020-A2-GN10	*Hotwire 5020 POTS Splitter Central Office Installation Instructions*
5030-A2-GN10	*Hotwire 5030 POTS Splitter Customer Premises Installation Instructions*
5038-A2-GN10	*Hotwire 5038 Distributed POTS Splitter Customer Premises Installation Instructions*
5038-A2-GN11	*Hotwire 5038 MVL POTS Filter Customer Premises Installation Instructions*
5620-A2-GN10	*Hotwire 5620 RTU Customer Premises Installation Instructions*
6020-A2-GZ40	*Hotwire 6020 MVL POTS Splitter Central Office Installation Instructions*
6038-A2-GN10	*Hotwire 6038 MVL POTS Filter Customer Premises Installation Instructions*
6310-A2-GN10	*Hotwire 6310 MVL Modem Customer Premises Installation Instructions*
8000-A2-GB22	*Hotwire Management Communications Controller (MCC) Card, IP Conservative, User's Guide*
8000-A2-GB27	*Hotwire DSLAM for 8310 MVL and 8510 RADSL Cards Network Configuration Guide*
8000-A2-GB90	*Hotwire 8100/8200 Internetworking Packet Concentrator (IPC) User's Guide*
8000-A2-GZ40	*Hotwire MCC Card, IP Conservative, Installation Instructions*
8310-A2-GZ40	*Hotwire 8310 MVL Card Installation Instructions*
8510-A2-GZ40	*Hotwire 8510 RADSL Card Installation Instructions*
8600-A2-GN20	*Hotwire 8600 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide*
8800-A2-GN21	*Hotwire 8800 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide*
8810-A2-GN20	*Hotwire 8810 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide*

Contact your sales or service representative to order additional product documentation.

Most Paradyne documents are also available on the World Wide Web at:

http://www.paradyne.com

Select *Service & Support* → *Technical Manuals*

Hotwire DSLAM System Description

1

What is the Hotwire DSLAM?

The Hotwire™ Digital Subscriber Line Access Multiplexer (DSLAM) is a Digital Subscriber Line (DSL) platform that houses a Management Communications Controller (MCC) card and up to 18 DSL cards. These can be 8310 Multiple Virtual Lines (MVL™) cards, 8510 Rate Adaptive Digital Subscriber Line (RADSL) cards, or a combination of both.

> **NOTE:**
>
> All references to DSL cards refer to both the 8510 RADSL and 8310 MVL cards, unless specifically noted otherwise.

The DSLAM interoperates with two types of Hotwire Service Nodes (SNs)/endpoints to deliver applications at high speeds in support of packet services over a DSL link.

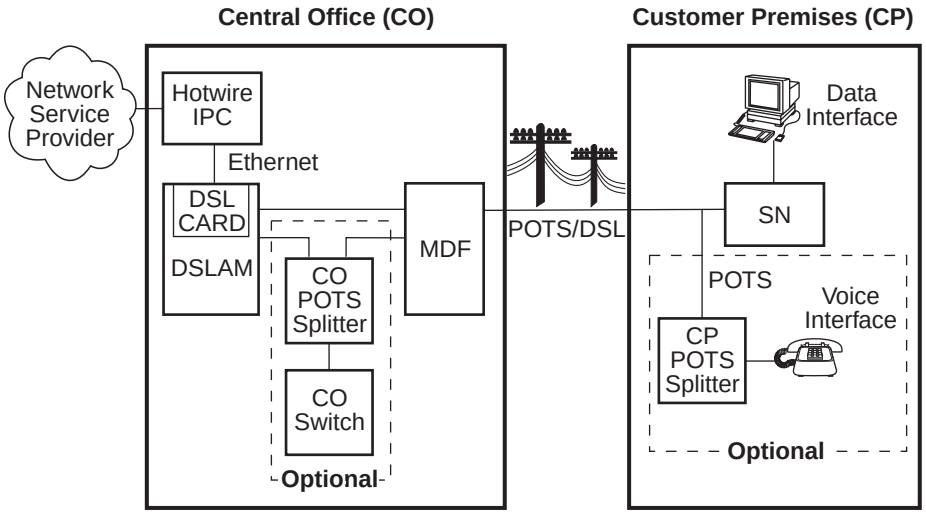
- The 8310 MVL card interoperates with the Hotwire 6310 MVL modem.
- The 8510 RADSL card interoperates with the Hotwire 5620 RTU (Remote Termination Unit).

The DSLAM is a set of central site products that terminate and consolidate packet data traffic from many customers in a serving area. It then forwards the traffic to one or more network access provider networks.

High-speed Internet and intranet access is bridged on the Layer 2 port cards and multiplexed over backbone networks. By enabling very high speeds using DSL technology and concentrating Internet Protocol (IP) traffic, greater performance is realized.

In addition, the Hotwire DSLAM with an endpoint such as a 6310 MVL modem and 5620 Service Node can co-exist with Plain Old Telephone Service (POTS) over the same copper telephone line, providing simultaneous usage of POTS and digital applications. That is, the optional central office (CO) POTS splitter and customer premises POTS filter allow simultaneous voice and data connections over a standard telephone line.

The following illustration shows a typical Hotwire configuration.



Legend: DSL - Digital Subscriber Line SN - Service Node
MDF - Main Distribution Frame POTS - Plain Old Telephone Service
IPC - Interworking Packet Concentrator

98-15974

Hotwire DSLAM Components

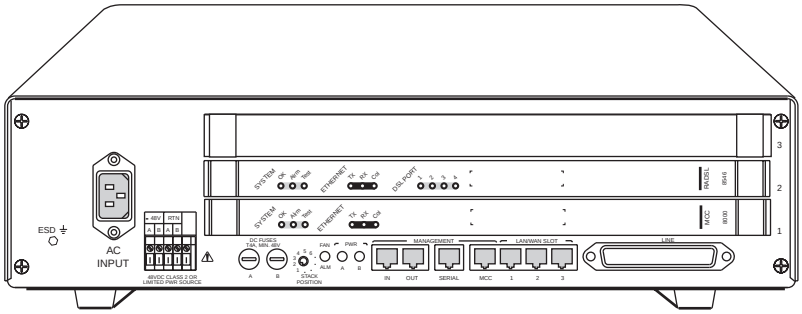
The minimum hardware requirements for a Hotwire DSLAM system consists of the following components:

- One Hotwire 8600, 8800, or 8810 DSLAM chassis
- One MCC card
- One 8310 MVL or 8510 RADSL card

Hotwire DSLAM Chassis

There are three types of chassis:

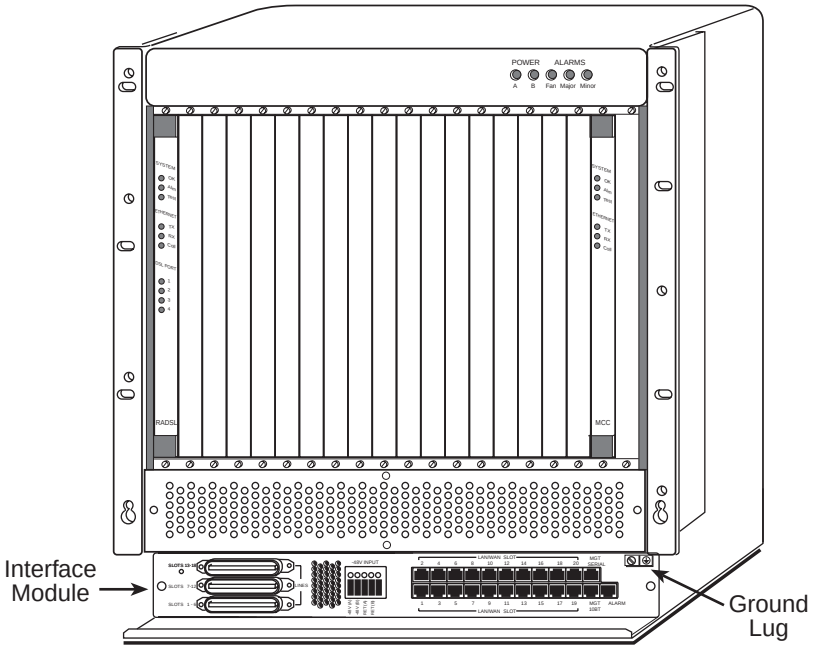
- The **Hotwire 8600 DSLAM** chassis is an independent, standalone system. The stackable design provides for up to six chassis to share management access through a single MCC card, which in turn, allows an additional slot for a DSL card in each of up to five additional chassis.



98-15350-02

In a stacked configuration, the first or base chassis must contain an MCC card in Slot 1. In addition to the MCC card, the base chassis can house up to two DSL cards. Each additional chassis in the stack houses up to three DSL cards. For more information, see the *Hotwire 8600 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide*.

- The **Hotwire 8800 DSLAM** chassis is a 20-slot chassis designed to house up to 18 DSL cards and one MCC card. (The remaining slot is reserved for the future use of a redundant MCC card.) For more information, see the *Hotwire 8800 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide*.
- The **Hotwire 8810 DSLAM** chassis is a higher density carrier, for use with new and future high-density cards. This 20-slot chassis with integral power, alarm, cooling, and interface subsystems is designed to house up to 18 DSL cards and one MCC card. (The remaining slot is reserved for the future use of a redundant MCC card.) For more information, see the *Hotwire 8810 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide*.



Front View of a Hotwire 8800 or 8810 DSLAM Chassis

99-15280-04

MCC Card

The chassis requires one MCC card, which is a processor card that administers and provides diagnostic connectivity to the DSL cards. It acts as a mid-level manager and works in conjunction with a Simple Network Management Protocol (SNMP) system, such as Paradyne's OpenLane™ DCE Manager for HP OpenView, via its LAN port. It gathers operational status for each of the DSL cards and responds to the SNMP requests. It also has a serial port for a local user interface to the DSLAM.

For more information, see the *Hotwire Management Communications Controller (MCC) Card, IP Conservative, User's Guide.*

RADSL or MVL Card

The chassis requires at least one RADSL or MVL card, which is a circuit card that contains four RADSL or MVL ports, an Ethernet interface to the Internet Service Provider (ISP), and a processor/packet forwarder. The processor/packet forwarder controls the endpoints and forwards the packet traffic via the Ethernet and RADSL or MVL interfaces. When the 8600 DSLAM chassis is fully populated with 5 expansion chassis, it provides a total of 68 RADSL or MVL modem ports. When the 8800 or 8810 DSLAM chassis is fully populated, it provides a total of 72 RADSL or MVL modem ports.

Hotwire DSLAM Features

The Hotwire DSLAM system contains the following features:

- High-speed Internet or intranet access
- RADSL ports
- MVL ports
- Subscriber authentication, security access, and permission features that prevent users from accessing unauthorized services
- Diagnostic tests and performance capabilities
- Primary network management support via SNMP agent for monitoring and traps
- Telnet for configuration and diagnostics

Levels of Access

There are two levels of diagnostic/administrative access in the Hotwire DSLAM system:

- **Administrator**

  The Administrator has complete read/write access to the DSLAM system. With Administrator permission, you can set specific parameters and variables to configure cards, ports, interfaces, Virtual Network ID (VNID) bridging, and endpoint selection.

- **Operator**

  The Operator has read-only access and can view configuration information and monitor performance but has no configuration menu access or modification permission.

Software Functionality

Depending upon your system access, you can:

- Configure the system,
- Monitor the system, and/or
- Run applications and diagnostic tests to troubleshoot the network.

Configuring the DSL Cards

The Hotwire DSLAM software provides DSL configuration options to:

- Configure the DSL cards
- Configure the interfaces and ports
- Set up user accounts
- Upload or download a copy of a card's configuration data to or from a Trivial File Transfer Protocol (TFTP) server
- Download a new version of the DSL and endpoint software

NOTE:

You must have Administrator permission to configure the system.

For more information about configuring the system, see Chapter 3, *Configuring the Hotwire DSLAM,* and Chapter 4, *8310 MVL and 8510 RADSL Card Configuration*.

Monitoring the DSL Cards

The Hotwire DSLAM software provides submenu options to monitor the activity of the Hotwire DSL cards. The monitoring screens allow you to:

- List the status of active ports and interfaces in a card, as well as display statistics about other physical layers and interfaces.
- Display network protocol statistics, such as information about an application program assigned to a specific socket number, UDP statistics, TCP data and connection statistics, IP statistics, ICMP packet statistics, and SNMP statistics including SNMP authentication statistics.
- Display information about the Client, ARP, and VNIDs.
- Display endpoint information about DSL Ports 1–4 such as Service Node type, system name, system contact, and system location. Model and serial number, along with firmware and hardware revisions, are also shown.

Use the monitoring screens to help you gather pertinent information and isolate potential problem areas. You can monitor the system with either Administrator or Operator permission.

For more information about monitoring the system, see Chapter 5, *Monitoring the Hotwire DSLAM*.

Troubleshooting and Diagnostics

The Hotwire DSLAM system provides DSL diagnostic submenu options that:

- Display self-test results for CPU health, memory and ports, and resets.
- Show major alarms such as Selftest Failure, Processor Failure, and DSL or Ethernet port failure.
- Show minor alarms such as Configuration Error or Incorrect SN ports.
- Run a nondisruptive packet echo test over the DSL line.

NOTE:

You must have Administrator permission to perform most of the troubleshooting and diagnostic activities. However, you can run nondisruptive tests as a user with Operator permission.

For more information about troubleshooting and diagnostics, see Chapter 6, *Diagnostics and Troubleshooting*.

NOTE:

If you would like more information on DSL-based services, applications, and network deployment, refer to Paradyne's *DSL Sourcebook.* The book may be downloaded or ordered through Paradyne's World Wide Web Site at **http://www.paradyne.com**.

Hotwire Menus and Screens

2

Overview

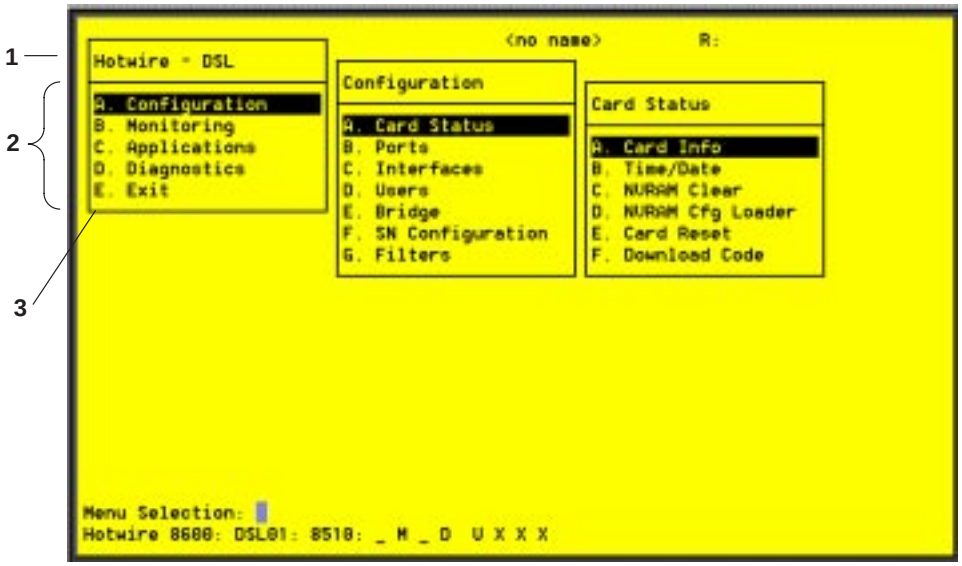
The Hotwire DSLAM has a menu- and screen-driven user interface system that enables the user to configure and monitor the Hotwire cards. This chapter contains:

Menu and Screen Formats

The Hotwire DSLAM uses an ASCII-based text format for its menus and screens. This section describes the components of a typical Hotwire menu and screen.

Components of a Hotwire Menu

A typical Hotwire menu format looks like this:

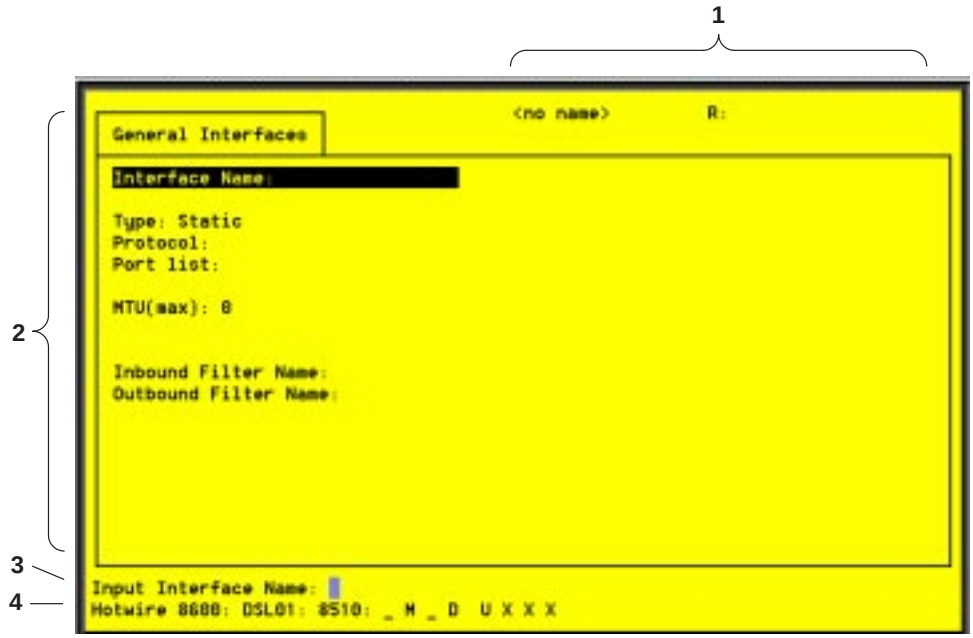


1. **Menu Title** is the top line of the menu window that displays the title of the menu or submenu.
2. **Menu List** is the portion of the menu window that displays the list of menu options. When selected, a menu option displays a submenu window or screen.
3. **Letter Navigation Keys** are provided within a menu list. These keys provide a convenient way (shortcut) to select a menu item.

   For example, from the Hotwire – DSL menu illustrated above, you can simply press the **A** key to select the Configuration menu item. The Configuration menu appears. You can then press the **A** key to select the Card Status menu item. This action displays the Card Status menu. (You can also use the arrow keys on your keyboard to select a menu item. See *Commonly Used Navigation Keys* on page 2-4 for more information.)

Components of a Hotwire Screen

A typical Hotwire screen looks like this:



1. **System Header Line** is the top line of the screen. This line has two fields that provide system login information.

   — The first field displays the system name or the individual card name. (Access the System Information screen by selecting the appropriate card in the chassis and then follow this menu sequence: *Configuration* → *Card Status* → *Card Info*.) If you do not define the system name, the DSLAM user interface will display **<no name>**.

   — The second field displays the current login. This field displays **R:<user_login>** where **R:** indicates a remote login and **<user_login>** is the login account of the user currently accessing the system. For example, if a user with a login account called *admin* logs into the system, this field will display **R:admin**.

2. **Display Area** is the top portion of the screen on which pertinent DSLAM system information is displayed. This is also the portion of the screen on which fields requiring input are displayed. However, you cannot enter values for the fields in this portion of the screen. You must enter field values in the Input Line at the bottom of the screen (see #3, below).

3. **Input Line** is the area of the screen where you are prompted to enter values for the specific field that is highlighted on the screen.

   For example, in the General Interfaces screen above, the Interface Name field is highlighted. If you want to modify an interface, you must enter the Interface Name at the **Input Interface Name:** prompt at the bottom of the screen.

4. **Status Line** is the last line on the screen. This line displays status information about the selected card. For information about these fields, see *Card Selection Screen* on page 2-10.

Commonly Used Navigation Keys

The following table lists navigation keys and their definitions. These commands are used to move around the Hotwire DSLAM menus and screens.

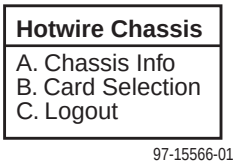
Keys	Definition
Ctrl-e	Returns to the Card Selection screen from any screen.
Ctrl-r	Resets counters (on monitoring statistics displays).
Ctrl-u	Clears the current input or prompt line.
Ctrl-v	Displays pop-up menus.
Esc h, ?	Displays the online Help screen.
Esc l, Ctrl-l	Refreshes the screen.
Esc n	Goes to the next window.
Esc p, Ctrl-z	Goes back to the previous window.
Esc t, Ctrl-a, Ctrl-c, Ctrl-t, or Ctrl-y	Goes back to the original, top-level window.
Left arrow, Ctrl-b	Moves the cursor to the left.
Right arrow, Ctrl-f	Moves the cursor to the right.
Up arrow, Ctrl-p	Moves up to the previous menu selection or entry field.
Down arrow, Ctrl-n	Moves down or to the next selection.
Enter or Return	Accepts entry.
Backspace, Del, Ctrl-d	Erases the character to the left of the prompt.

Hotwire Menu Hierarchy

This section describes the menu structure of the Hotwire user interface.

Hotwire Chassis Main Menu

The following illustration shows the Hotwire Chassis Main Menu.



97-15566-01

From the Hotwire Chassis Main Menu, you can select:

- **A. Chassis Info** to enter or display chassis information, such as the chassis name, name of person responsible for the system, and physical location of the chassis.
- **B. Card Selection** to select a particular card in the chassis. This screen also displays status information about all cards in the chassis. The card you select determines which Hotwire menu the system will display next (Hotwire – DSL menu).

  For more information, see *Card Selection Screen* on page 2-10.
- **C. Logout** to exit from the current login session on the Hotwire DSLAM.

  For more information, see *Exiting from the System* on page 2-12.

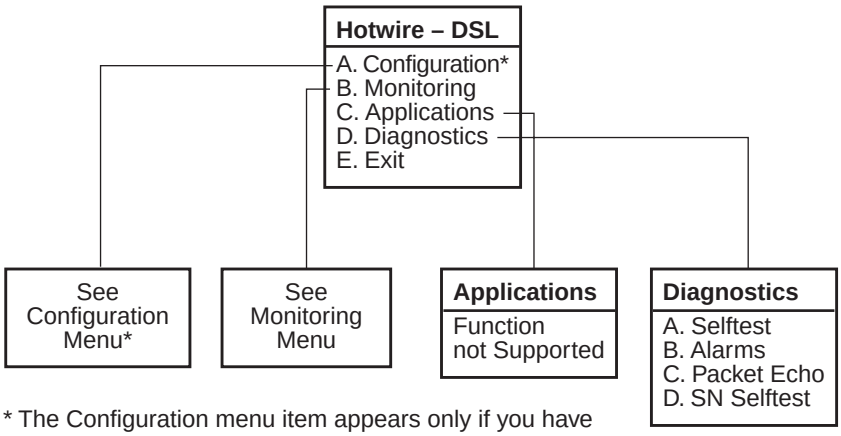
Hotwire – MCC Menu

After selecting the MCC card from the Card Selection screen, the DSLAM system displays the Hotwire – MCC Menu. From this menu, you can configure, monitor, run applications, and troubleshoot the MCC card.

For information on the MCC card, see the *Hotwire Management Communications Controller (MCC) Card, IP Conservative, User's Guide.*

Hotwire – DSL Menu

After selecting a specific DSL card from the Card Selection screen, the DSLAM system displays the Hotwire – DSL Menu.

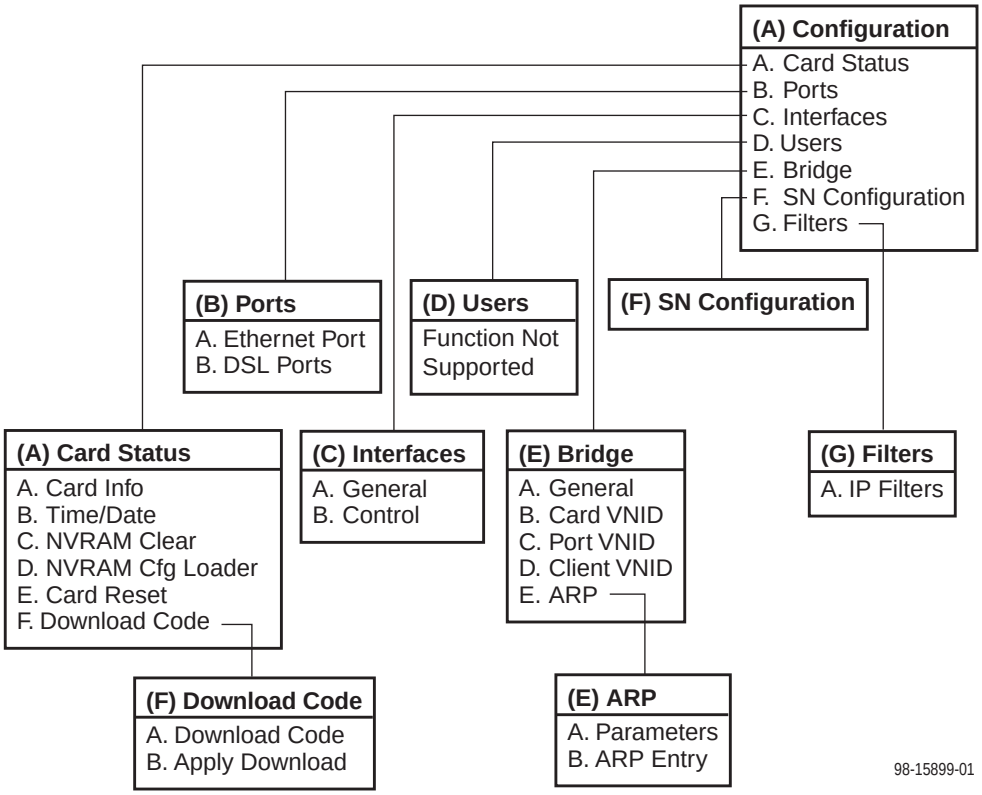


* The Configuration menu item appears only if you have Administrator permission.

From this menu, you can configure, monitor, run applications, and troubleshoot a specific DSL card.

DSL Card Configuration Menu

The following figure illustrates the complete Configuration menu hierarchy from the Hotwire – DSL menu.

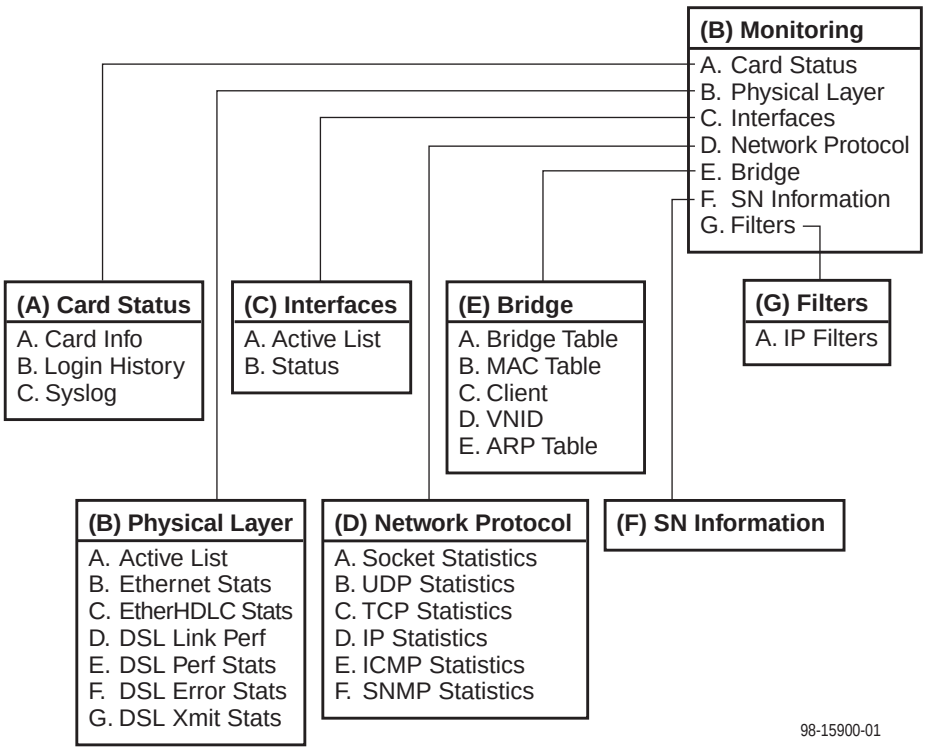


NOTE:

The Configuration menu and its submenus appear only when logging in to the system with a user account that has Administrator permission.

DSL Card Monitoring Menu

The following figure illustrates the complete Monitoring menu hierarchy from the Hotwire – DSL menu.



Logging In to the System

This section describes how to log in to the Hotwire DSLAM system after the system has been configured for the first time.

NOTE:

When you power on the system for the first time, the system displays the Who Am I screen. This screen can be accessed only from the local console.

Reviewing the Levels of Access

There are two levels of privileges on the Hotwire DSLAM system. Your user accounts can be configured with a user name, password, and privilege of:

- Administrator, giving you access to all of the features of the system including configuration options, or
- Operator, giving you read-only access.

The default access is no login and password with Administrator status. To provide login security to the DSLAM, user accounts must be configured.

NOTE:

There must be at least one Administrator configured in order to have system security.

For information on configuring user accounts, see the *Hotwire Management Communications Controller (MCC) Card, IP Conservative, User's Guide.*

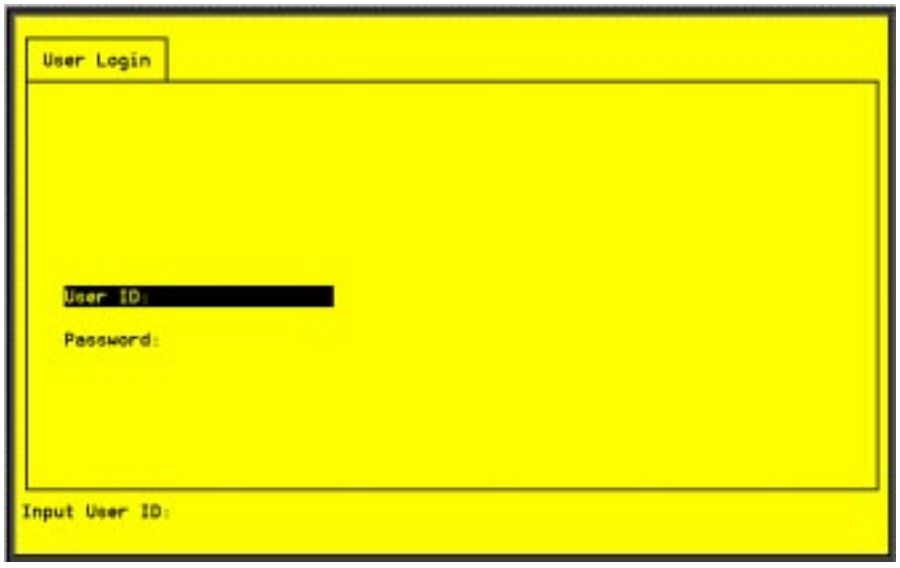
User Login Screen

You can log in to the Hotwire DSLAM system using either a local VT100-compatible terminal or a remote Telnet connection. However, the Hotwire DSLAM system accepts only one login session at a time.

At the User Login screen, enter your login ID and password.

NOTE:

The User Login screen only appears if one or more users have been defined.



NOTE:

The login ID and password are case-sensitive; that is, the system recognizes both upper- and lowercase letters. For example, if you enter your user name and password information in uppercase letters and your assigned user name and password are in upper- and lowercase letters, the system will not let you log in.

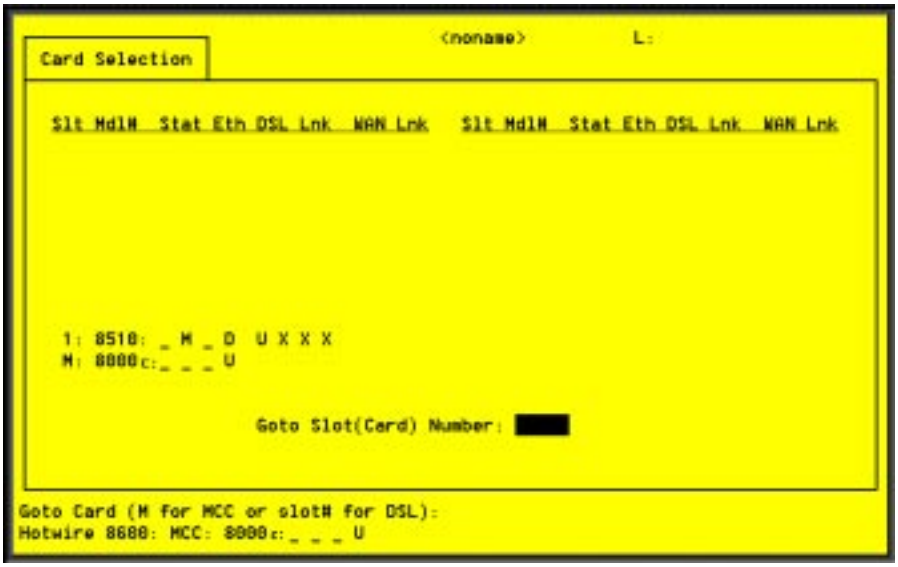
After entering your login ID and password, the system displays the Hotwire Chassis Main Menu.

Card Selection Screen

From the Hotwire Chassis Main Menu, select Card Selection to display the status of any of the 18 DSL cards installed in the chassis by type and slot number. The Card Selection screen also displays general and interface status for each card.

NOTE:

The Card Selection screen for the Hotwire 8800 chassis appears slightly different from the 8600 shown below.



The status of each DSL card is indicated by codes displayed in any of eight positions to the right of the card selected.

The following table explains the valid codes by position.

Column Heading	Position	Display	Description
Slt	<slot number>		M = MCC card 1–18 = slot number for DSL card
Mdl #	<card type>		First four digits of the card model number: 8310 = MVL card 8510 = RADSL card 8000c = MCC card (conservative)
Stat	1	T or _	Test mode. Card currently in test mode or _ for no active test.
	2	M or _	Major alarm. Major alarm present on card or _ for no active major alarm.
	3	R or _	Minor alarm. Minor alarm present on card or _ for no minor alarm active.
Eth	4	U, D, or X	Status of Ethernet link: U=Up, D=Down, X=Disabled
DSL Lnk	5, 6, 7, & 8	U, D, X, or H	Status of DSL card Port 1–4 link: U=Up, D=Down, X=Disabled, or H=Handshaking
WAN Lnk	For future Use.		

For example, if you select DSL card in Slot 1, the following may be displayed:

```
1: 8510  _  M  _  D  U  X  X  X
Position:  1  2  3  4  5  6  7  8
```

This display shows the following:

- There is an 8510 card in Slot 1
- Position 1 – No current test (_)
- Position 2 – Major alarm is present (M)
- Position 3 – No minor alarm present (_)
- Position 4 – Ethernet link is Down (D)
- Position 5 – DSL port 1 is Up (U)
- Positions 6, 7, and 8 – DSL ports 2, 3, and 4 are disabled (X)

On the Card Selection screen, there is a prompt used to select a specific card in the DSLAM chassis. When a DSL slot number is entered, you are connected to the card you selected.

For more information about the status displayed on this screen, such as major and minor alarms, see *Troubleshooting* in Chapter 6, *Diagnostics and Troubleshooting.*

Accessing the Hotwire – DSL Menu

▶ Procedure

To access the Hotwire – DSL menu:

1. From the Hotwire Chassis Main Menu, select Card Selection.

   The Card Selection screen appears.

2. Verify that the DSL card you want to access appears on the Card Selection screen. (See *Card Selection Screen* on page 2-10 for more information.)

3. At the **`Goto Card (MCC or DSLnn):`** prompt, enter the number of the slot. Then, press Enter. For example, if you want to configure the DSL card in Slot 13, type **13**.

   The Hotwire – DSL menu appears.

Exiting from the System

You can manually log out of the system or, after five minutes of inactivity, the system will automatically log you out.

Manually Logging Out

▶ Procedure

To exit from the Hotwire DSLAM system:

1. Return to the Card Selection screen by selecting Exit from either the Hotwire – MCC menu or the Hotwire – DSL menu.

2. Press Ctrl-z.

3. From the Hotwire Chassis Main Menu, select Logout.

   The system exits from the current login session on the Hotwire DSLAM.

Automatically Logging Out

The DSLAM system has an automatic timeout feature that logs you out of the system after five minutes of inactivity. You will need to log back in to continue your work.

To log back in, press Enter to display the User Login screen and log in.

Configuring the Hotwire DSLAM

3

Overview

The Hotwire DSLAM enables you to configure and manage the Hotwire MCC and DSL cards. This chapter describes the basic card configuration instructions.

Domain Types

To monitor and control the overall system, the Hotwire Access Network should be partitioned into two distinct domains:

- **Service domain(s) (Layer 2)**
- **Management domain (Layer 3)**

It is recommended that the management domain reside in a separate domain from the service domain for security purposes and to improve download performance.

Service Domain

The service (or data) domain is comprised of all clients and servers (grouped physically or virtually) that communicate across a common WAN or LAN connection for internet access. This is the Layer 2 bridging domain of the NSP. The Access Node cards and the Service Nodes are the Hotwire components of this domain. The service domain encompasses an NSP and all end-user systems that subscribe to that NSP.

Management Domain

The primary function of the management domain is monitoring and configuring the network. The management domain resides in a mutually exclusive domain from that of the service (data) domains. The MCC card functions as a service router and is the primary tool for configuring and diagnosing the management domain.

Configuring the DSL Cards

Use the procedures in the following order to minimally configure DSL cards for user data connectivity. For detailed information on these instructions, see Chapter 4, *8310 MVL and 8510 RADSL Card Configuration*.

For information about MCC and DSL card network topologies, consult the *Hotwire DSLAM for 8310 MVL and 8510 RADSL Cards Network Configuration Guide*. To configure the MCC card, refer to the *Hotwire Management Communications Controller (MCC) Card, IP Conservative, User's Guide*.

The following table lists optional steps to configure the VNID for the DSL card.

For each DSL card, to . . .	**See . . .**
1. Configure VNID(s) on a RADSL or MVL card	*Configuring VNID(s) on a DSL Card*, page 3-3.
2. Select the active VNID on each RADSL or MVL port	*Configuring the Active VNID on each DSL Port*, page 3-4.
3. Configure static users	*Configuring Static Users*, page 3-5.
4. Configure IP filter rules	*Configuring IP Filter Rules*, page 3-7.

Configuring VNID(s) on a DSL Card

▶ Procedure

To configure at least one VNID for this RADSL or MVL card from the Hotwire – DSL Card menu:

1. Follow this menu selection sequence*:*

   Configuration → *Bridge* → *Card VNID* (**A-E-B**)

2. Type **0** or press Enter at the **`Item Number (0 to add new record):`** prompt.

3. Enter the VNID at the **`Enter VNID ID between 2 and 4094 or space to delete:`** prompt.

4. Enter **enabled** at the **`Enabled/Disabled:`** prompt in the Mux Fwd field. (Default = enabled.)

5. Enter **disabled** at the **`Enabled/Disabled:`** prompt in the IP Filter field. (Default = disabled.)

6. Enter **enabled** at the **`Enabled/Disabled:`** prompt in the IP Scoping field. (Default = enabled.)

7. If desired, enter an ISP domain name at the **`Domain Name:`** prompt.

   Example: If entering a VNID for XYZ Company, enter **XYZ** as the Domain Name.

8. Enter **yes** at the **`yes/no:`** prompt to save your changes.

NOTES:

For more information about the fields listed above, see Table 4-4, Bridge Options, in Chapter 4, *8310 MVL and 8510 RADSL Card Configuration.*

Also, refer to *Service Domain* in the *Hotwire DSLAM for 8310 MVL and 8510 RADSL Cards Network Configuration Guide.*

Configuring the Active VNID on each DSL Port

You can configure multiple VNIDs with different next hop routers with one active VNID configured per port.

▶ Procedure

To configure the active VNID on each RADSL or MVL port from the Hotwire – DSL menu:

1. Follow this menu selection sequence:

   Configuration → *Bridge* → *Port VNID* (**A-E-C**)

2. Enter the port number at the **`DSL Port #:`** prompt.
3. Enter **`a`** (to activate) at the **`Action(Edit/Activate/Deactivate):`** prompt.
4. Enter the number of the VNID to be assigned to this port at the **`Input Number:`** prompt. If you want a VNID that spans several RADSL or MVL cards, you must specify the same VNID number across all cards.

   Activate each port separately.
5. Press Ctrl-z and save the changes.

NOTES:

For more information about the fields listed above, see Table 4-4, Bridge Options, in Chapter 4, *8310 MVL and 8510 RADSL Card Configuration.*

Configuring Static Users

▶ Procedure

From the Hotwire – DSL menu:

1. Follow this menu selection sequence:

   Configuration → *Bridge* → *Client VNID* (**A-E-D**)

2. Enter the port number at the **`DSL Port #:`** prompt.
3. Type **`0`** or press Enter at the **`Input Number:`** prompt.
4. Enter the IP Address of this user at the **`Enter Client IP address (nnn.nnn.nnn.nnn):`** prompt.
5. Enter the subnet mask at the **`Enter Subnet Mask (nnn.nnn.nnn.nnn):`** prompt.
6. Enter the IP address of the next hop router for this client at the **`Enter IP address of next hop router (nnn.nnn.nnn.nnn):`** prompt.
7. Enter the VNID for this user at the **`Input VNID ID:`** prompt.
8. Enter **`yes`** at the **`yes/no:`** prompt to save your changes.

NOTES:

For more information about the fields listed above, see Table 4-4, Bridge Options, in Chapter 4, *8310 MVL and 8510 RADSL Card Configuration.*

For information on configuring dynamic users, see *Service Domain* in the *Hotwire DSLAM for 8310 MVL and 8510 RADSL Cards Network Configuration Guide.*

Addressing a Location Using DHCP

When IP Scoping is enabled, DHCP scoping is also enabled. The DSLAM intercepts IP ARP and DHCP transaction messages.

- DHCP clients in one VNID domain can only obtain the IP addresses in one IP subnet, and the router's primary IP address is part of that subnet. As a result, DHCP clients in one VNID domain cannot be in different subnets.
- If the DHCP scope falls in a statically configured subnet, all the dynamic clients will get an IP address in that static subnet.

There are three ways to locate IP addresses with DHCP:

- Dynamically provisioned host addresses (each entry is associated with lease time)
- Statically configured subnets with no lease time (dynamic clients obtain IP addresses within this subnet)

Configuring Subnet Addressing

To define a subnet entry, the IP address has to be entered as the lower boundary address of the subnet. Otherwise, only a host entry can be configured.
For example, a subnet with a mask of 255.255.255.192 requires one of the following IP addresses:

- 255.255.255.0
- 255.255.255.64
- 255.255.255.128
- 255.255.255.192

NOTE:

For more information about the fields listed above, see Table 4-6, Filters Options, in Chapter 4, *8310 MVL and 8510 RADSL Card Configuration.*

Configuring Subnet Masks

After the IP address is entered, a default subnet mask is displayed. The default subnet mask is based on the IP address entered and can be changed.

If the IP Address entered is . . .	Then the Default Subnet Mask is . . .
*xxx.xxx.xxx.*0	255.255.255.0
*xxx.xxx.*0.0	255.255.0.0
*xxx.*0.0.0	255.0.0.0
xxx.xxx.xxx.xxx	255.255.255.255

To configure the DSL card, a valid subnet must be used. When a Host entry is input, any valid IP address results in a subnet mask of 255.255.255.255.

When a Subnet entry is entered, the valid subnet mask is based on the IP address entered. A valid subnet mask must be in one of the following formats:

- 255.0.0.0
- 255.*nnn.*0.0
- 255.255.*nnn.*0
- 255.255.255.*nnn*

  Where *nnn* must be: 0, 128, 192, 224, 240, 248, 252, 254.

NOTE:

For more information about the fields listed above, see Table 4-4, Bridge Options, in Chapter 4, *8310 MVL and 8510 RADSL Card Configuration.*

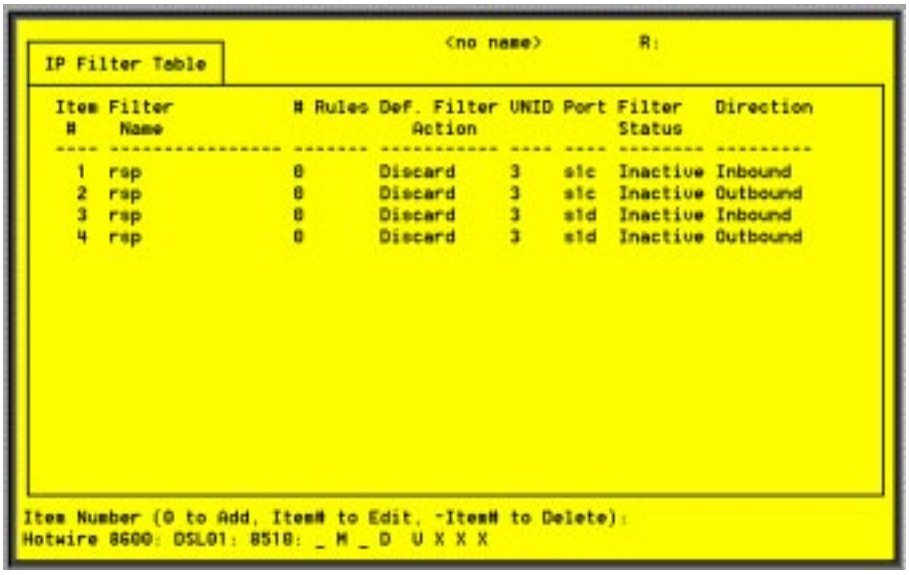
Configuring IP Filter Rules

▶ Procedure

Configure IP Filters and associated rules in the following sequence:

1. Define each filter. An IP filter consists of a set of rules.
2. Configure rules for each filter. TCP/UDP/ICMP traffic types can be selectively forwarded or discarded based on the conditions specified in the rule.
3. Bind the filter to the interface using the General Interfaces screen (**A-C-A**).

   This is an example of data contained in the IP Filter Table.



   — An inbound filter acts on packets in the upstream direction from the client to the NSP server.

   — An outbound filter acts on packets in the downstream direction from the NSP server to the client.

To configure the IP Filter attributes and rules, refer to *DSL Configuration Filters Screen* in Chapter 4, *8310 MVL and 8510 RADSL Card Configuration.*

8310 MVL and 8510 RADSL Card Configuration

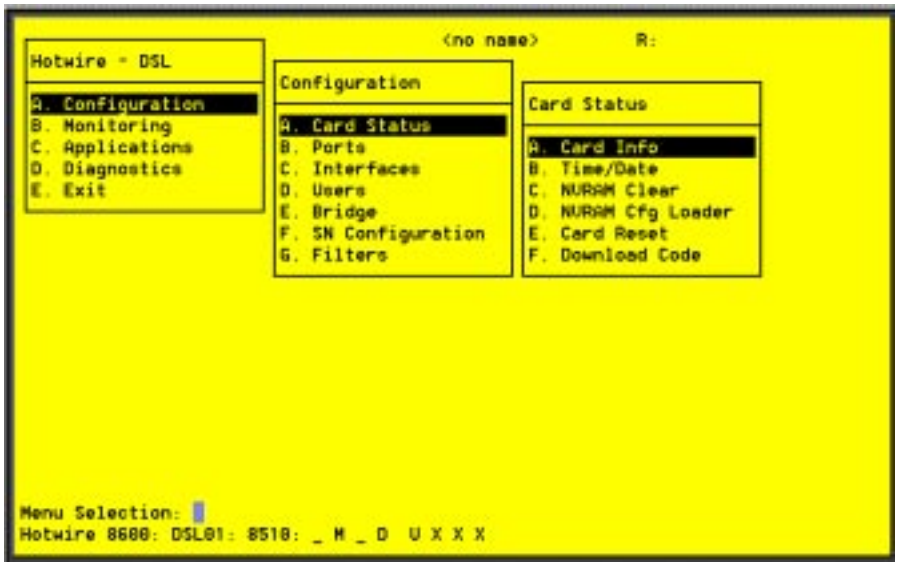
4

Overview

This chapter describes configuration options on the DSL card. Use these options to customize your applications. For information on customizing the MCC card, see the *Hotwire Management Communications Controller (MCC) Card, IP Conservative, User's Guide.*

DSL Configuration Card Status Screens

Use the system information submenu of the Card Status screens to configure basic DSL card-level information.



NOTE:

Only a user who logs in to the Hotwire DSLAM with Administrative permission can configure the DSL card.

▶ Procedure

To configure card information, time/date, clear NVRAM, upload or download configuration sets, download new firmware, or reset card:

1. Follow this menu selection sequence:

   Configuration → *Card Status* (**A-A**)

2. The Card Status menu appears. Enter the desired value on each selected screen and field as shown in Table 4-1 and press Enter.

Table 4-1. Card Status Options (1 of 3)

Card Info (Card Information)	**A-A-A**
Gives the user the ability to configure basic card-level information. **Card Name** – 16 alphanumeric characters. Name assigned to the card. **Card Contact** – 32 alphanumeric characters. Name or number of party responsible for card. **Card Location** – 16 alphanumeric characters. Location assigned to the card. **Local Control Terminal Port Mode** – Standard/Extended (Default = Standard). Standard is for USA keyboards; Extended is for European keyboards. **Remote Control Terminal Port Mode** – Standard/Extended (Default = Standard). Standard is for USA keyboards; Extended is for European keyboards.	
Time/Date	**A-A-B**
Gives the user the ability to view the time zone, local time, and date on the DSL card. **Time zone** – Name of your time zone. **Local Time/Date** – Time in *hh.mm* format (am or pm). Date in *mm/dd/yy* format. NOTE: At system boot time, the time zone, local time, and date on the DSL cards automatically synchronizes with the MCC card.	
NVRAM Clear	**A-A-C**
Gives the user the ability to clear out the Non-Volatile RAM (NVRAM) in order to reuse the card or to reconfigure the current card. CAUTION: If you select yes on this screen, you will permanently remove all of the configuration information you have stored on this card. The system will perform a reset and return to the factory configuration.	

Table 4-1. Card Status Options (2 of 3)

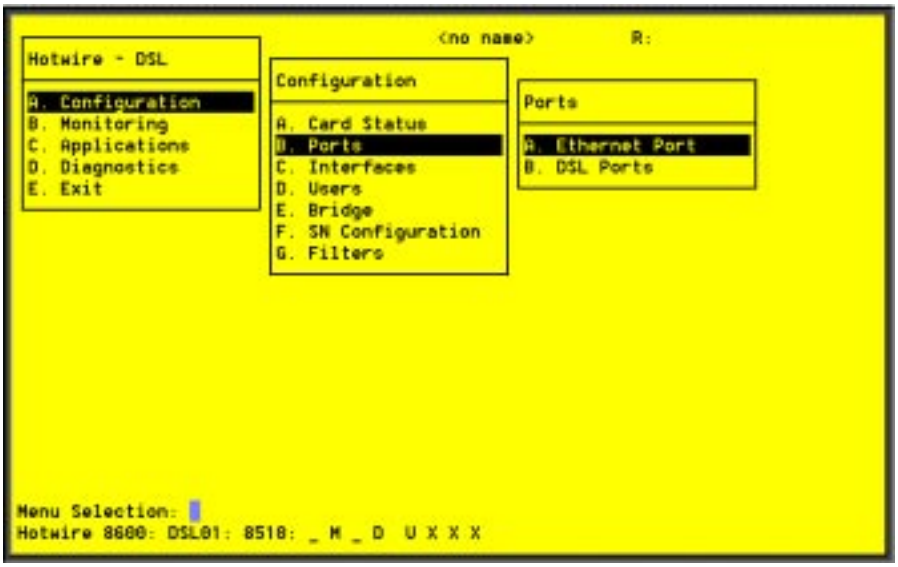
NVRAM Cfg Loader (NVRAM Configuration Loader)	**A-A-D**
Gives the user the ability to upload or download a copy of the card's binary configuration data to or from a Trivial File Transfer Protocol (TFTP) server. **Configuration File Name** – The file name may be a regular path name expression of directory names separated by a forward slash (/) ending with the file name. The total path name length must be less than 40 characters. If the TFTP server is hosted by a DOS machine, then directory and file names must follow the 8.3 naming convention imposed by DOS. **DOS Machine** If your server is hosted by a DOS machine, you must name the file to be uploaded using the DOS convention 8-character length. The system will automatically upload the configuration file and create directories and file names as needed. **UNIX Machine** If your server is hosted by a UNIX machine, the configuration file you name **will not** be created on the UNIX system by the TFTP server. It is **critical** that you work with your system administrator to plan the naming conventions for directories, file names, and permissions so that anyone using the system has read and write permissions. (This is a UNIX system security feature). NOTE: This must be done before you can upload files to a UNIX server. **TFTP Server IP Address** – Address in *nnn.nnn.nnn.nnn* format. This address must be in the management domain. **TFTP Transfer Direction** – Upload-to-Server/Download-to-Server (Default = Upload-to-Server). Select Upload-to-Server to store a copy of the card's configuration on the server. Select Download-to-Server to have the file server send a copy of the stored configuration file to the card. **Start Transfer** – Yes/No (Default = No). **Packets Sent** – Number of packets sent in download. **Packets Received –** Number of packets received in download. **Bytes Sent** – Number of bytes sent in download. **Bytes Received** – Number of bytes received in download. **Transfer Status** – Status of the upload or download transfer. NOTE: After a download, the card must be reset for the new configuration to take effect.	
Card Reset	**A-A-E**
Gives the user the ability to reset the card. This resets all counters and if a new configuration or software version has been downloaded, the new code will then become active. NOTE: This action disrupts the data flow for at least 30 seconds.	

Table 4-1. Card Status Options (3 of 3)

Download Code (Download Code and Apply Download)	**A-A-F (A and B)**
Gives the user the ability to download a new version of code and apply the downloaded code. For further information on this feature, see Appendix A, *Download Code*. **Download Code (A)** or **Apply Download (B)**	
Download Code (A) This screen is similar to the NVRAM Configuration Loader screen (**A-A-D**). **Image File Name** – The file name may be a regular path name expression of directory names separated by a forward slash (/) ending with the file name. The total path name length must be less than 40 characters. If the TFTP server is hosted by a DOS machine, then directory and file names must follow the 8.3 naming convention imposed by DOS. **TFTP Server IP Address** – Address in *nnn.nnn.nnn.nnn* format. This address must be in the management domain. **Start Transfer** – Yes/No (Default = No). **Packets Sent** – Number of packets sent in download. **Packets Received** – Number of packets received in download. **Bytes Sent** – Number of bytes sent in download. **Bytes Received** – Number of bytes received in download. **Transfer Status** – Status of the download transfer. Once the download is complete, press Ctrl-z to exit back to the Download Code submenu and select Apply Download.	
Apply Download (B) This selection applies the downloaded code and drops all connections by performing a device reset. This screen is used to overlay the previously downloaded image for the card. If you select yes at the Reset System prompt, the system goes through a system restart and interrupts service on the card. For further information on this feature, see Appendix A, *Download Code*. NOTE: If you have not previously downloaded code, then you will not be able to access this selection.	

DSL Configuration Ports Screens

Use the system information submenu of the Ports screens to display the DSL Ports screen.



▶ Procedure

To configure ports:

1. Follow this menu selection sequence:

   Configuration → *Ports* (**A-B**)

2. The Ports menu appears. Enter the desired value on each selected screen and field as shown in Table 4-2 and press Enter.

Table 4-2. Ports Options (1 of 3)

Ethernet Port	**A-B-A**
Gives the user the ability to select full- or half-duplex on the Ethernet Port.	
Port Name – Enter the port name (up to 7 characters).	
Full Duplex – Enable/Disable (Default = Disable).	
Function – Edit/Reset. Select Reset to have changes become active.	

Table 4-2. Ports Options (2 of 3)

DSL Ports (RADSL Parameters) 8510 RADSL Card	A-B-B

Gives the user the ability to configure the operational and alarm parameters of the RADSL ports on the RADSL 8510 card. Each RADSL port is configured separately.

NOTE: For the 8310 MVL card, refer to the DSL Ports (MVL Parameters) 8310 MVL Card section at the end of this table.

Action – Edit/Reset. Edit to configure the DSL ports, Reset to reset the port and make changes active.

Port # – Enter Port 1–4 (Default = 0).

Tx Power – 0 dB, –3 dB, –6 dB. Enter the rate that allows you to reduce the transmit power by: –3 dB or –6 dB (Default = 0 dB). Short loops require less power, reducing crosstalk and giving better performance on longer loops in the same cable bundle.

SN Tx Power – 0 dB, –3 dB, –6 dB, –9dB (Default = –6 dB).

Startup Margin – The Startup Margin (SM) field is used to determine the quality of the connection of the upstream link on system startup. It is used in conjunction with the adaptive speed fields to determine the initial line speeds of the DSL link. The value is between –3 and 9. In Adaptive Mode, if the margin falls below SM, the DSL link will be restarted at a slower speed. If the calculated margin of the next speed is greater than SM by 3 dB, the speed will increase. Enter –3 to 9 (Default = 3).

Reed-Solomon Interleaving – Long/Short (Default = Long).

Behavior – Fixed/Adaptive (Default = Adaptive). In fixed rate mode, the DSL port will operate at the specified upstream and downstream speed. In rate adaptive mode, the rates will not exceed the maximum speed and traps are sent when the links drop below the minimum, as the transmission characteristics of the loop change.

SN Type – Model number of endpoint. For Model 8510 RADSL Card, SN type is 5620. (This field is read-only.)

Fixed: Down Speed* – 7168/6272/5120/4480/3200/2688/2560/2240/1920/1600/1280/1024/960/896/768/640/512/384/256 (Default = 2560 kbps).

Fixed: Up Speed* – 1088/952/816/680/544/408/272/91 (Default = 1088 kbps). Enter the fixed upstream speed.

Adaptive: Max Dn Speed* – 7168/6272/5120/4480/3200/2688/2560/2240/1920/1600/1280/1024/960/896/768/640/512/384/256 (Default = 7168 kbps). Enter the maximum downstream speed.

Adaptive: Min Dn Speed* – 7168/6272/5120/4480/3200/2688/2560/2240/1920/1600/1280/1024/960/896/768/640/512/384/256 (Default = 640 kbps). Enter the minimum downstream speed.

Adaptive: Max Up Speed* – 1088/952/816/680/544/408/272/91 (Default = 1088 kbps). Enter the maximum upstream speed.

Adaptive: Min Up Speed* – 1088/952/816/680/544/408/272/91 (Default = 408 kbps). Enter the minimum upstream speed.

Margin Threshold Offset: – Sends a trap message if the margin on either end falls below the startup margin by the selected value. Enter a value for the margin threshold trap (–7 dB to +14 dB, or D to Disable). (Default = +3).

Example: With a startup margin of +3 dB and a threshold offset of +3 dB, the Low Margin Trap will be sent if the margin falls below 0 dB.

Link Down Ct: – Sends a trap message if the number of DSL link down events in 15 minutes exceeds the selected value. Enter a value for the Link Down Count Trap (0 to 1000, or D to Disable). (Default = 0.)

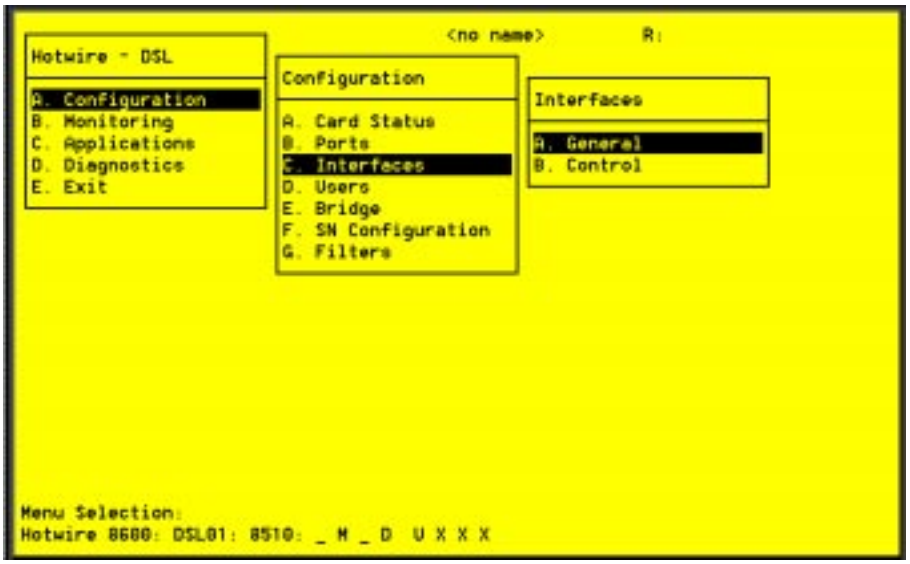
NOTE: If you have made changes to this screen, select Reset in the Action field to make the changes active.

* If you select a downstream speed of 2560 or higher, your upstream speed selection is limited to 1088/952/680/408.

Table 4-2. Ports Options (3 of 3)

DSL Ports (MVL Parameters) 8310 MVL Card	A-B-B
Gives the user the ability to configure the operational and alarm parameters of the MVL ports on the 8310 card. Each MVL port is configured separately. NOTE: For the 8510 RADSL card, refer to the previous section of this table, DSL Ports (RADSL Parameters) 8510 MVL Card. **Action** – Edit/Reset. Use Edit to configure the MVL ports. Use Reset to reset the port and make changes active. **Port #** – Enter Port 1–4 (Default = 0). **Behavior** – Adaptive. In rate adaptive mode, the rates will vary between the minimum and maximum speeds as the transmission characteristics of the loop change. **Max Speed** – 768/704/640/576/512/448/384/320/256/192/128 kbps (Default = 768). **SN Type** – Model number of endpoint. For Model 8310 MVL Card, SN type is 6310. (This field is read-only.) **Margin Threshold:** – Sends a trap message if the margin on either end falls below the selected value. Enter a value for the margin threshold trap (–5 dB to +10 dB) (Default = +3). Enter D to disable trap. **Link Down Ct:** – Sends a trap message if the number of MVL link down events in 15 minutes exceeds the selected value. Enter a value for the Link Down Count Trap (0 — 1000). Enter D to disable trap. (Default = 0.) NOTE: If you have made changes to this screen, select Reset in the Action field to make the changes active.	

DSL Configuration Interfaces Screens



Use the system information submenu of the Interfaces screens to configure basic interface information.

▶ Procedure

To view DSL card information, configure Maximum Transmission Unit (MTU) settings, bind filters to DSL interfaces, or restart, stop, or monitor an interface:

1. Follow this menu selection sequence:

   Configuration → *Interfaces* (**A-C**)

2. The Interfaces menu appears. Enter the desired value on each selected screen and field as shown in Table 4-3 and press Enter.

Table 4-3. Interfaces Options

General (General Interfaces)	**A-C-A**
Gives the user the ability to configure and view basic card interface information about a given interface, including binding filters. **Interface Name** – 3 characters. e1a = Ethernet port; s1c, s1d, s1e and s1f = RADSL or MVL interface. **Type** – Static or Dynamic interface type. **Protocol** – HDLC or Ethernet. Interface protocol. **Port List** – Ports available on the card. **MTU (max)** – 64–1600 bytes (Default = 1536). Receipt of packets above the MTU setting will be dropped. NOTE: The above MTU values are the only values you may enter. Make certain that if you change from the default value, the new numbers are appropriate to your network. Do a card reset or reset the Ethernet interface. **Inbound Filter Name** – Enter the filter name with a maximum of 12 characters. This field appears only if the DSL interface selected is s1c–s1f. To view a list of configured inbound filters, press Ctrl-v. NOTE: An inbound filter acts on packets in the upstream direction from the client to the NSP server. **Outbound Filter Name** – Enter the filter name with a maximum of 12 characters. This field appears only if the DSL interface selected is s1c–s1f. To view a list of configured outbound filters, press Ctrl-v. NOTE: An outbound filter acts on packets in the downstream direction from the NSP server to the client.	
Control (Control Interfaces)	**A-C-B**
Gives the user the ability to start, stop, and monitor (up, down, or testing) the current state of an interface. NOTE: Stopping the interface disables all of the traffic on that port, including diagnostics. If you want to disable only customer traffic, disable all VNIDs on that port. There are no user-configurable elements on this screen except for the ability to start and stop the interface. Valid choices for the DSL card are e1a, s1c, s1d, s1e, and s1f.	

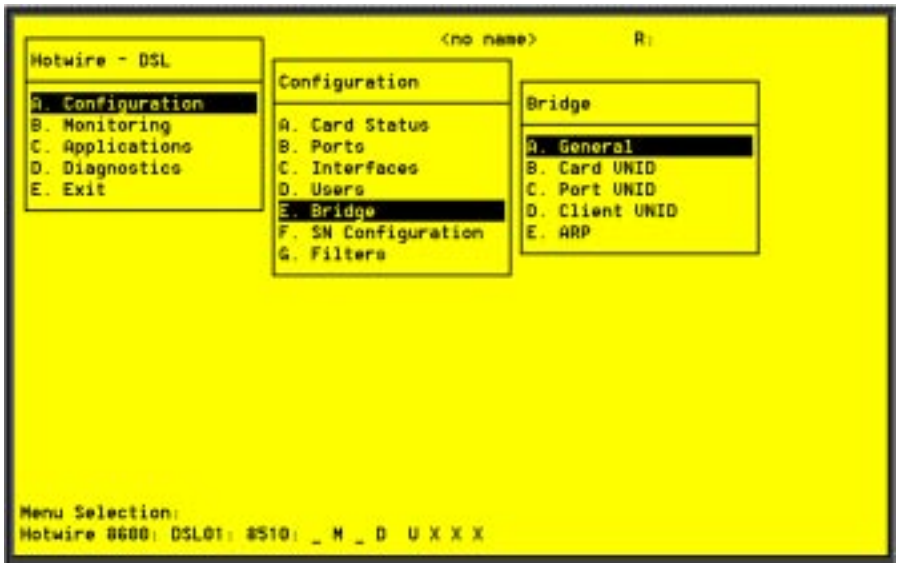
DSL Configuration Users Screens

Use the system information submenu of the Users screens to configure login accounts for Telnet sessions directly to the DSL cards.

This menu item is not currently supported on this card.

DSL Configuration Bridge Screens

Use the system information submenu of the Bridge screens to configure bridging information.



▶ Procedure

1. Follow this menu selection sequence:

   Configuration → *Bridge* (**A-E**)

2. The Bridge menu appears. Enter the desired value on each selected screen and field as shown in Table 4-4 and press Enter.

Table 4-4. Bridge Options (1 of 3)

General (General Bridge Parameters)	**A-E-A**
Gives the user the ability to configure general bridge parameters. **Complete Entry Timeout** – Enter the bridge aging timeout (10–1,000,000 seconds) (Default = 300). **VNID Tagging** – Enable/Disable VNID tagging on the card.	
Card VNID	**A-E-B**
Gives the user the ability to configure Virtual Network IDs (VNIDs) for the entire card. There are a maximum of 16 entries per card. **Item** – Enter 0 (zero) to add a new record. **VNID** – Enter a VNID between 2–4094 (Default = Null). **Mux Fwd** – Enable/Disable (Default = Enable). ■ When Mux Fwd is enabled, all upstream traffic is sent out the 10BaseT interface. Forwarding restrictions are set by the other parameters on the screen. ■ When Mux Fwd is disabled, the DSLAM forwards traffic based on a destination MAC address. Either enabled or disabled, traffic is forwarded on ports having the same VNID designation. **IP Filter** – Enable/Disable (Default = Disable). ■ When IP filtering is enabled,the DSLAM looks at IP traffic from the subscriber to authenticate the source IP address. ■ When IP filtering is disabled, no source authentication check is performed. **IP Scoping** – Enable/Disable (Default = Enable). ■ When IP Scoping is enabled, DHCP scoping is also enabled and the DSLAM intercepts IP ARP and DHCP transaction messages. ■ When IP Scoping is disabled, DHCP client entries are not added to the Client table and non-IP traffic is forwarded. NOTE: For additional information on DHCP, refer to Chapter 3, *Configuring the Hotwire DSLAM*. **Domain Name** – Enter the domain name of the Internet Service Provider (ISP).	
Port VNID	**A-E-C**
Gives the user the ability to configure one VNID association on an individual port. **DSL Port #** – Enter the DSL port number (Default = 1). **VNID** – Number of the VNID port (Default = none). This field is read-only. **Default NHR** – Enter the IP address of the next hop router (NHR) in *nnn.nnn.nnn.nnn* format (Default = none). If the NHR IP address does not exist for that port, a default NHR IP address is used. If the default NHR IP address does not exist, the Address Resolution Protocol (ARP) request is ignored.	

Table 4-4. Bridge Options (2 of 3)

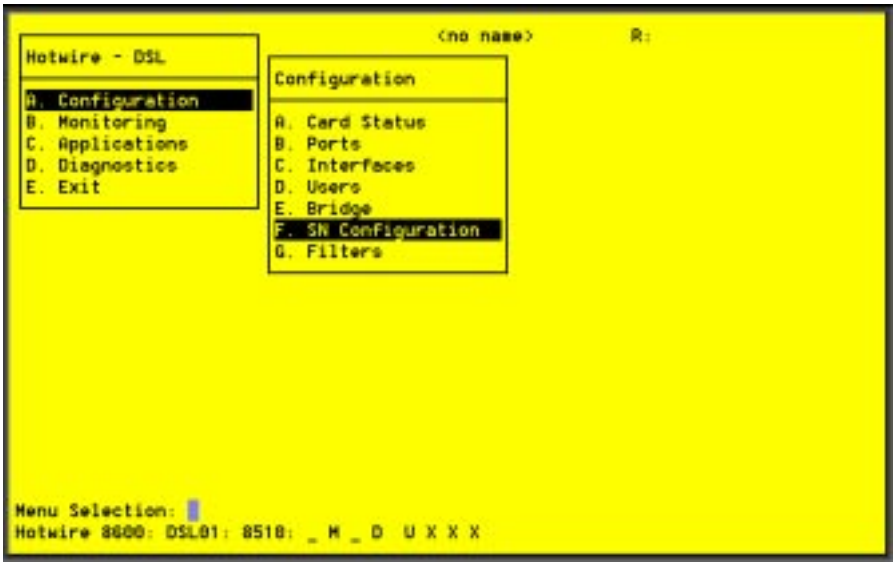
Client VNID	**A-E-D**
Gives the user the ability to configure static clients on VNIDs. Up to 32 entries per port (static users, DHCP users, or subnets) are allowed. Multiple screens are required to completely configure the port. For a list of VNID, press Ctrl-v. **DSL Port #** – Enter the DSL port number 1–4 (Default = 1). **Item** – Enter 0 to add a new client or enter an existing entry number to edit this entry. **IP Address** – For single users, enter the client IP address in *nnn.nnn.nnn.nnn* format (Default = none). There must be an entry in this field. Typically, all IP addresses in the same VNID would be on the same subnet. NOTE: For additional information, refer to *Configuring Subnet Masks* in Chapter 3, *Configuring the Hotwire DSLAM.* **Subnet Mask** – For multiple users with IP addresses in the same subnet, enter both the IP address and the subnet mask in *nnn.nnn.nnn.nnn* format. CAUTION: The same subnet cannot be assigned to multiple ports. An error message will appear if the IP address of the next hop router is not in the same subnet as the client IP address. Geographically dispersed clients are supported through static host-specific entries only. **NHR** – Enter the IP address of the next hop router in *nnn.nnn.nnn.nnn* format, if different than the default for the VNID (Default = none). **VNID** – VNID ID between 2–4094 (This field is read-only.) **Type** – S = Static or D = Dynamic (This field is read-only.) NOTE: If a DHCP response cannot be added to the host table because it already has 32 entries, and if IP scoping/filtering has been enabled on the Card VNID screen (**A-E-B**), any subsequent upstream packets from that host are dropped.	

Table 4-4. Bridge Options (3 of 3)

ARP (Parameters and Add ARP Entry)	**A-E-E (A and B)**
Select **Parameters (A)** or **ARP Entry (B)**	
Parameters (A) Gives the user the ability to configure general Address Resolution Protocol (ARP) cache parameters. **Complete Entry Timeout (minutes)** – Length of time that a complete entry remains in the ARP Table before removal. A complete entry is one for which there is a MAC address and a node has responded to the ARP request. Range = 1–200,000 minutes (Default = 20). **Incomplete Entry Timeout (minutes)** – Length of time in minutes that an incomplete entry remains in the ARP table before being removed. (An incomplete entry is an entry without a MAC address.) This is also the amount of time that a packet will remain in the system while waiting for address resolution. Range = 1–255 minutes (Default = 3). NOTE: If you have made changes to this screen, you must do a card reset for the changes to be in effect.	
ARP Entry (Add ARP Entry) (B) Gives the user the ability to add entries into the ARP cache. **Item** – Enter 0 (zero) to add a new record. **IP Address** – *nnn.nnn.nnn.nnn* format. **MAC Address** – *xx-xx-xx-xx-xx-xx* format. **VNID** – Enter a VNID ID between 2–4094 (Default = Null). There must be an entry made in this field. **Trailer** – Yes/No (Default = No). **Perm** – Yes/No (Default = No). If you select Yes for Permanent and No for Proxy, the ARP entry will be saved in NVRAM (up to 32 entries). These are loaded when the card resets. NOTE: For the Add ARP Entry (B) screen, all other information entered is not stored in the non-volatile memory and will be lost when you reset the card.	

DSL Configuration Service Node Screens

Use the SN Configuration screen to configure endpoint Service Node information.



▶ Procedure

1. Follow this menu selection sequence:

   Configuration → *SN Configuration* (**A-F**).

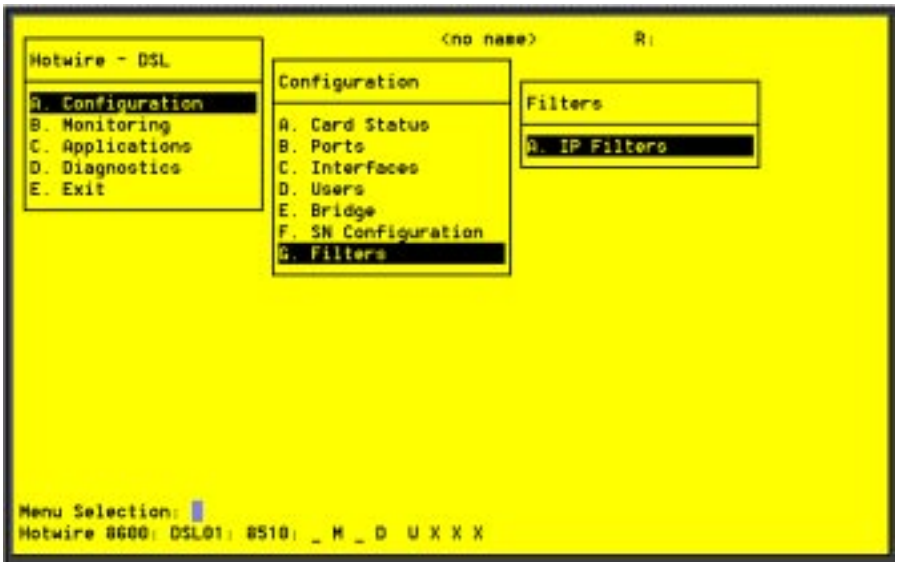
2. The SN Configuration menu appears. Enter the desired value on the selected screen and field as shown in Table 4-5 and press Enter.

Table 4-5. Service Node Options

SN Configuration	A-F
Displays endpoint information for the 5620 RTU or 6310 MVL modem.	
Port # – Enter the RADSL or MVL port number (1–4).	
SN Type – Model number of SN connected to the DSL port. For Model 8510 RADSL, the SN is 5620. For Model 8310 MVL, the SN is 6310. (This field is read-only.)	
System Name – 16 alphanumeric characters. Enter the name assigned to the SN.	
System Contact – 32 alphanumeric characters. Enter the name or number of the person responsible for the SN.	
System Location – 16 alphanumeric characters. Enter the location of the SN.	
Model Num – Model number of card. (This field is read-only.)	
Serial Num – Serial number of card. (This field is read-only.)	
Firmware Rev – Version of firmware. (This field is read-only.)	
Hardware Rev – Version of hardware. (This field is read-only.)	
CAP Rev – Version of CAP chipset for Model 8510 RADSL card only. (This field is read-only.)	
MVL Rev – Version of MVL chipset for Model 8310 MVL card only. (This field is read-only.)	
Reset SN? – Yes/No. Enter yes to reset the SN and begin a self-test.	
NOTE: Entering yes in the Reset SN field will temporarily disrupt the data path on the specified DSL port while the SN resets.	
SN Selftest Results – Pass/Fail. This field displays the results of the SN self-test, when completed.	

DSL Configuration Filters Screen

Use the IP Router Filters to add, delete, or edit a filter.



▶ Procedure

1. Follow this menu selection sequence:

   Configuration → *Filters* → *IP Filters* (**A-G-A**).

2. The IP Filters screen appears. Enter the desired value on the selected screen and field as shown in Table 4-6 and press Enter.

Table 4-6. Filters Options (1 of 2)

IP Filters (IP Filter Table)	**A-G-A**
The IP Filter Table screen displays the following information: **Item #** – Enter a value from 1–8 to add, delete, or modify individual filter entries. **Filter Name** – Name of the IP filter. (This field is read-only.) **# of Rules** – Number of rules in the IP filter. (This field is read-only.) **Def filter action** – Forward/discard. Default filter action. (This field is read-only.) **VNID** – Interface and VNID to which the filter belongs. (This field is read-only.) **Port** – Port to which the filter belongs: s1c–s1f. (This field is read-only.) **Filter status** – Active/Inactive (Default = Inactive). (This field is read-only.) **Direction** – Inbound/Outbound. (This field is read-only.) On the bottom of this screen, at the **`Item Number (0 to Add, # to Edit, –# to Delete)`** prompt: ■ Select 0 (zero) to add a new filter. ■ Select # (*n*) to edit existing filters. Example: Enter 3 to add Filter #3. ■ Select -# (–*n*) to delete a filter. Example: Enter –6 to delete Filter #6. The Add or Edit selection takes you to the IP Filter Configuration screen. When you exit that screen, you return to the IP Filters screen. NOTE: Deleting the filter deletes all the rules associated with that filter.	
IP Filters (IP Filter Configuration screen)	**A-G-A**
Allows you to build multiple rules for an IP filter. A filter consists of a set of rules applied to a specific interface to indicate whether a packet received or sent out of that interface is forwarded or discarded. You can add, edit, or delete filter rules within a named set. A filter works by successively applying the rules to the information obtained from the packet header until a match is found. The filter then performs the action specified by the rule on that packet, which forwards or discards the packet. If all the rules are searched and no match is found, the configured default filter action is executed. Host rules have higher precedence than network rules. Rules apply to the source/destination IP address, source/destination port number, and traffic types, such as TCP/UDP/ICMP. TCP/UDP/ICMP traffic is forwarded or discarded based on the conditions specified in the rule, including source and/or destination address and source and/or destination port number. You can have up to 33 rules per filter. Each rule reduces the packet throughput of the DSL card. There can be 8 filters per DSL card with a maximum of two filters per DSL port, one inbound filter and one outbound filter. The same filter can be applied as an inbound filter and an outbound filter. Filters are configured on the port card and the processing takes place on the endpoint. NOTE: Once your rules have been configured, you can then bind and activate the filter on the DSL interface using the *Configuration* → *Interfaces* → *General* screen (**A-C-A**).	

Table 4-6. Filters Options (2 of 2)

IP Filters (IP Filter Configuration) (*continued*)	**A-G-A**

Filter Name – Up to 12 characters.

Default Filter Action – Forward (Packet)/Discard (Packet) (Default = Forward). The Default Filter Action applies when there is no match or the filter has no rules configured.

DHCP Filter Action – Forward (Packet)/Discard (Packet) (Default = Forward). Forwards or discards DHCP transaction traffic on a particular DSL port.

Rule # – Up to 33 rules can be configured for each filter. The rule number is automatically assigned. The rules are reviewed sequentially. The most common rules should be entered first.

Source Address – *nnn.nnn.nnn.nnn* format. Enter valid host or network IP address. If 0.0.0.0 is entered, Source Comparison is ignored.

NOTE: For additional information, refer to *Configuring Subnet Addressing* in Chapter 3, *Configuring the Hotwire DSLAM.*

Source Mask – *nnn.nnn.nnn.nnn* format. If you specify a source subnet mask of 0.0.0.0, the system skips the source address comparison.

Source Comparison – Enabled/Disabled (Default = Disabled). When Source Comparison is disabled, the comparison is ignored.

Source Port # – 0–65535 (Default = 0).

Comparison Type (for source information) – Ignore – Do not do a comparison. To do a comparison on the port number specified in the packet and the rule, specify one of the following: Ignore – Ignore ports, EQ – Equal to, NEQ – Not Equal to, GT – Greater than, LT – Less than, In_Range – Within the specified range, Out_Range – Outside of the specified range (Default = Ignore).

Max. Source Port No. – 0–65535. Appears only when the source comparison type is In Range or Out of Range.

Destination Address – *nnn.nnn.nnn.nnn* format.

Destination Mask – *nnn.nnn.nnn.nnn* format. If you specify a destination subnet mask of 0.0.0.0, the system skips the destination address comparison.

Destination Comparison – Enabled/Disabled (Default = Disabled). When Destination Comparison is disabled, the comparison is ignored.

Destination Port # – 0–65535 (Default = null).

Comparison Type (for destination information) – Ignore – Ignore ports, EQ – Equal to, NEQ – Not Equal To, GT – Greater than, LT – Less than, In_Range – Within the specified range, Out_Range – Outside of the specified range.

Max. Destination Port No. – 2–65535. Appears only when the destination port comparison type is In Range or Out of Range.

Action – For a rule, TCP, UDP, or ICMP traffic will be forwarded or discarded provided other conditions have been satisfied.

- TCP – Forward/Discard (Default = Forward).
- UDP – Forward/Discard (Default = Forward).
- ICMP – Forward/Discard (Default = Forward).

Delete Rule – Yes/No (Default = No).

Monitoring the Hotwire DSLAM

5

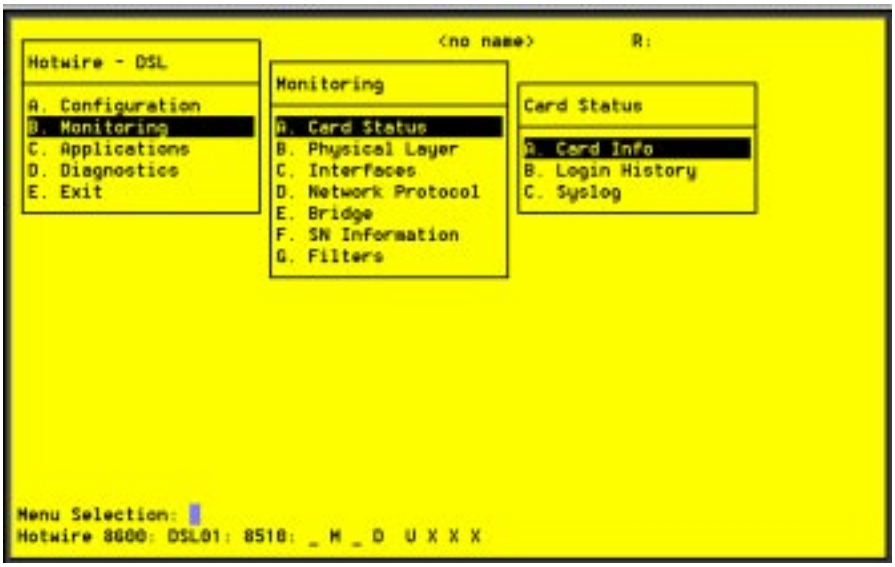
Overview

The Hotwire DSLAM lets you monitor the activity of the Hotwire DSL cards. When you select Monitoring from the Hotwire DSL Main Menu, a menu tree of selections on history and error logs, performance statistics, card status, and physical and logical interface status information is presented.

Most of the Monitoring screens are read-only; that is, the information displayed is to help you gather pertinent information and isolate potential problem areas. For diagnostic tools and hardware and software troubleshooting techniques, see Chapter 6, *Diagnostics and Troubleshooting*.

DSL Monitoring Card Status Screens

Use the Card Status screens to display read-only system information.



▶ Procedure

To view general card information, login history, and the system log:

1. Follow this menu selection sequence:

   Monitoring → *Card Status* (**B-A**)

2. The Card Status menu appears. Select the submenu option as shown in Table 5-1 and press Enter.

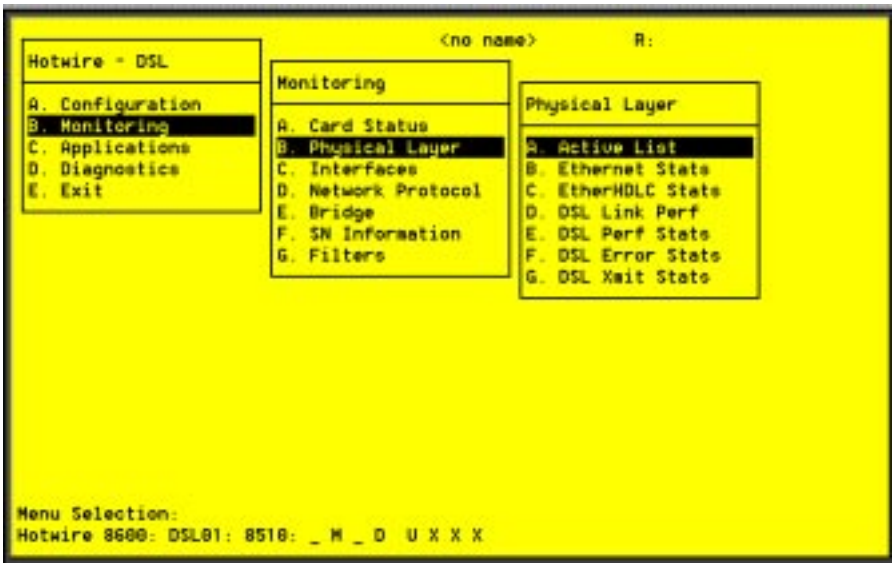
Table 5-1. Card Status Options

Card Info (General Card Information)	**B-A-A**
Displays card information. **Card Name** – Name assigned to the card. **Card Location** – Physical location of the system. **Card Contact** – Name or number of the person responsible for the card. **Card Up Time** – Length of time the card has been running. **Available Buffers** – Number of Buffers not in use. **Buffer Ram Size** – Size of the Buffer Ram. **Fast Data Ram Size** – Total and Available Fast Data Ram. **Card Type** – Type of Card (MCC, DSL). **Model Num** – Model number of card. **Serial Num** – Serial number of card. **Firmware** – Version of firmware. **CAP Firmware** – Version CAP chipset for Model 8510 RADSL card only. **MVL Rev** – Version of MVL chipset for Model 8310 MVL card only. **Hardware Rev** – Version of hardware.	
Login History	**B-A-B**
Displays a list of information on the 10 most recent logins. **User** – User ID. **Time** – Date and time of the most recent login. **Local/Remote** – Local or Remote Connection. **Number of unsuccessful Console logins** – Number of console logins that were incorrect in the last 10 attempts**.** **Number of unsuccessful Telnet logins** – Number of Telnet logins that were incorrect in the last 10 attempts.	
Syslog (System Log)	**B-A-C**
Displays a time stamped sequential list of operational type errors by date and error. There is one logged error per line in a downward scrolling list. The list has a 17-error entry maximum. When the log is full, the oldest entry is deleted. Refer to the Syslog Screen Example.	

Syslog Screen Example

DSL Monitoring Physical Layer Screens

Use the Physical Layer screens to display read-only system information about physical ports.



▶ Procedure

To view the active ports list, Ethernet statistics, and HDLC bus statistics:

1. Follow this menu selection sequence:

   Monitoring → *Physical Layer* (**B-B**)

2. The Physical Layer menu appears. Select the submenu option as shown in Table 5-2 and press Enter.

Table 5-2. Physical Layer Options (1 of 6)

Active List (Active Ports List)	**B-B-A**
Displays a list of the current status of all the active ports (e1a = Ethernet; s1c, s1d, s1e, and s1f = DSL cards). **Num** – Number of the port. **Name** – Name of the port. **Description** – Type of port. **MAC Address** – MAC address of the active port. (Internal dummy address used for non-Ethernet ports.) **Status** – In-use or disconnected.	

Table 5-2. Physical Layer Options (2 of 6)

Ethernet Stats (Ethernet Statistics)	**B-B-B**

Displays a list of the Ethernet statistics of the LAN port (e1a).

The counters increment in real time and you may press Ctrl-r at any time to reset the counters.

Port – Type of port (e1a).

Initialized Ethernet Ports – e1a (There is only one other net port on the card).

LAN Address – LAN (or MAC) address of the Ethernet port.

Bytes received – Number of bytes received by the Ethernet port since the last reset.

Bytes transmitted – Number of bytes transmitted by the Ethernet port since the last reset.

Packets received – Number of packets received by the Ethernet port since the last reset and what type.

- Multicast – Single packets copied to a specific subset of network addresses.
- Broadcasts – Messages sent to all network destinations.
- Flooded – Information received, then sent out to each of the interfaces.
- Filtered – Processes or devices that screen incoming information.
- Discarded – Packets discarded.
- VNID Error – Number of errors transmitted by the VNID and what type.

Errors – Number of errors transmitted by the Ethernet port and what type.

- M = Multi-collision frames – not counted in this release and always set to 0.
- L = Late collisions – collision detected often; at least 64 bytes have been transmitted.
- E = Excessive collisions – port tried to send a packet 15 times without success.
- Overruns – No buffer space.
- Bad CRC – Cyclic Redundancy Check.
- Framing – Receiver improperly interprets set of bits within frame.
- Jumbo gram – Ethernet packet too long.
- Overflow – Part of traffic that is not carried.
- Buffer – No buffer space.

Fast restarts – Number of fast restarts and what type (RX off, TX off, Mem err).

Endless Pkt – Number of endless packets received on the Ethernet port.

Startless Pkt – Number of startless packets received on the Ethernet port.

Babble – Number of garbled packets received due to crosstalk.

Table 5-2. Physical Layer Options (3 of 6)

Ethernet Stats (Ethernet Statistics) (continued)	**B-B-B**
Packets transmitted – Number of packets transmitted by the Ethernet port and what type. ■ Multicast – Single packets copied to a specific subset of network addresses. ■ Broadcast – Messages sent to all network destinations. ■ Flooded – Information received, then sent out to each of the interfaces. ■ Local origin – Locally transmitted packet; e.g. Ping. ■ Queued – Packets waiting to be processed. **Errors** – Number of errors transmitted by the Ethernet port and what type. ■ M = Multi-collision frames – not counted this release and always set to 0. ■ L = Late collisions – collision detected often; at least 64 bytes have been transmitted. ■ E = Excessive collisions – port tried to send a packet 15 times without success. **Disconnects** – Number of disconnects on the Ethernet port and what type. ■ Disable – Transmit error, timed out. ■ MAU drop – Transceivers dropped. ■ Xmit fail – Transmit fail.	
EtherHDLC Stats (EtherHDLC Statistics)	**B-B-C**
Displays statistics in real time on the HDLC link later protocol between the Access Node and each Service Node (s1c, s1d, s1e, and s1f ports.) (See field definitions from previous screen.) The counters increment in real time and you may press Ctrl-r at any time to reset the counters. **Port name** – Port name (s1c, s1d, s1e, or s1f). **Initialized EtherHDLC Ports** – s1c, s1d, s1e, or s1f. **Bytes received** – Number of bytes received. **Bytes transmitted** – Number of bytes transmitted. **Packets received** – Number of packets received. **Packets transmitted** – Number of packets transmitted. **Errors** – Number of other receive errors. (If a high number of errors have been received, the card may have to be reset.)	

Table 5-2. Physical Layer Options (4 of 6)

DSL Link Perf (DSL Link Performance Summary)	B-B-D
Displays a summary of the link performance for each of the DSL ports. Enter port number 1–4 to see the fields for current 15-minute period (real time count of events during the past 0 to 15 minutes), previous 15-minute period (data updated every 15 minutes), previous 1-hour period (data updated every hour), and 24-hour period (data is updated every hour). **Port # :** – Enter the port number (1–4) you wish to monitor. **Dn Margin** – Measure of the noise margin on the specified port in the downstream direction. A positive margin number reflects a lower error rate with a higher tolerance. **Up Margin** – Measure of the noise margin on the specified port in the upstream direction. A positive margin number reflects a lower error rate with a higher tolerance. **DnErrRate** – This statistic is not available for this release and 0 (zero) appears for each time period. **UpErrRate** – Block error rate in the upstream direction. Error rate = bad blocks/good blocks and is expressed as A x 10^{-B}. **DnAttEst** – Measure of the downstream transmission loss on the DSL line. **UpAttEst** – Measure of the upstream transmission loss on the DSL line. **link dn count** – Number of times the DSL link has gone down. **elp lnk up** – Count of the elapsed time in seconds that the link has been up. **elp time** – Count of the elapsed time in seconds since the DSL card was last reset. **Pct link up** – Percentage of time the DSL link has been up in the past 24 hours.	

Table 5-2. Physical Layer Options (5 of 6)

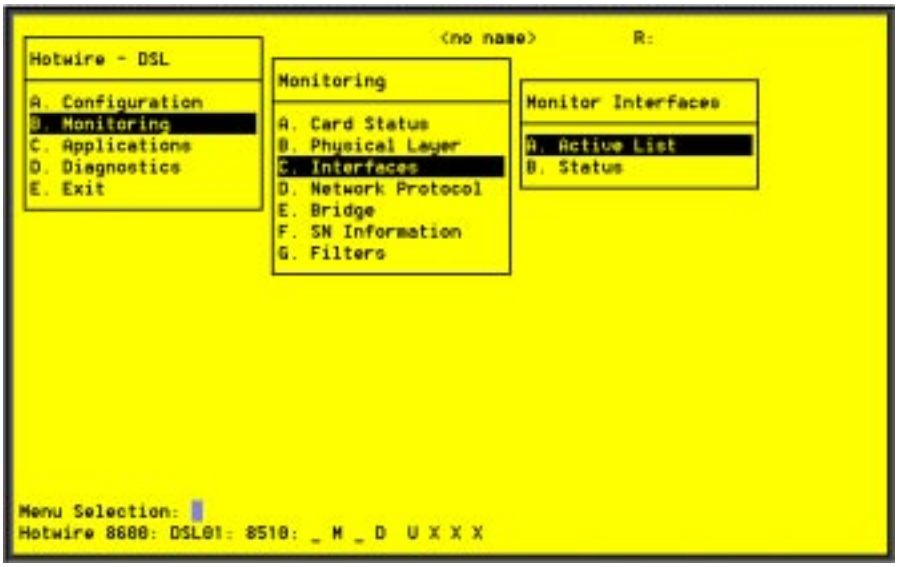
DSL Perf Stats (DSL Performance Stats)	B-B-E
Displays the link performance for each of the DSL ports. Tells you the number of times the link has been down and the elapsed time the link has been up. Enter port number 1–4 to see the fields for current 15-minute period (real time count of events during the past 0–15 minutes), previous 15-minute period (data updated every 15 minutes), previous 1-hour period (data updated every hour), and 24-hour period (data updated every hour). **Port # :** – Enter the port number (1–4) you wish to monitor. **15min Valid** – Number of 15-minute intervals in which downstream performance data has been received across the DSL link from the endpoint (SN). **pkt rcv dn** – Number of downstream packets received. **pkt snt dn** – Number of downstream packets sent. **pkt lost dn** – Number of downstream packets lost. **pkt rcv up** – Number of upstream packets received. **pkt snt up** – Number of upstream packets sent. **pkt lost up** – Number of upstream packets lost. **k octs sent dn** – How many thousands of octets have been sent to the SN. **k octs rcv dn** – How many thousands of octets have been received by the SN. **k octs sent up** – How many thousands of octets have been sent upstream from the SN. **k octs rcv up** – How many thousands of octets have been received upstream from the SN. **Customer Data** **k octs sent dn** – How many thousands of octets have been sent downstream. **k octs sent up** – How many thousands of octets have been received upstream.	

Table 5-2. Physical Layer Options (6 of 6)

DSL Error Stats	**B-B-F**
Displays the error performance (margin) rates for each of the DSL ports after selecting a specific DSL port number. Margin is a measure of performance. Enter port number 1–4 to see the fields for current 15-minute period (real time count of events during the past 0–15 minutes), previous 15-minute period (data updated every 15 minutes), previous 1-hour period (data updated every hour), and 24-hour period (data bucket updated every hour). A margin of 0 db equals an expected bit error rate of 10^{-7}. (The higher the margins, the fewer the errors.) The counters increment in real time and you may press Ctrl-r at any time to reset the counters. **dn margin** – Measure of the noise margin on the specified port in the downstream direction. A positive margin number reflects a lower error rate with a higher tolerance. **up margin** – Measure of the noise margin on the specified port in the upstream direction. A positive margin number reflects a lower error rate with a higher tolerance. **dn err rate** – This statistic is not available for this release and an NA appears for each time period. **up err rate** – Block error rate in upstream direction. Error rate = bad blocks/good blocks and is expressed as A x 10^{-B}. **dn err secs** – Count of the number of down error seconds with at least one block error in the downstream data path. **up err secs** – Count of the number of up error seconds with at least one block error in the upstream data path. **dn svr err sec** – Count of the number of seconds with at least 800 block errors in the downstream data path. **up svr err sec** – Count of the number of seconds with at least 800 block errors in the upstream data path.	
DSL Xmit Status (DSL Transmit Stats)	**B-B-G**
Displays the transmit and receive statistics for each of the DSL ports after selecting a specific DSL port number. Enter port number 1–4 to see the fields for current 15-minute period (real time count of events during the past 0–15 minutes), previous 15-minute period (data updated every 15 minutes), previous 1-hour period (data updated every hour), and 24-hour period (data updated every hour). The counters increment in real time and you may press Ctrl-r at any time to reset the counters. **Port #** – Enter the port number (1–4) you wish to monitor. **dn xmit pwr** – Measure of the power level of the downstream signal sent to the SN (in db). **up xmit pwr** – Measure of the power level of the upstream signal sent by the SN (in db). **dn rx gain** – Measure of how much amplification was applied to the signal received at the SN. **up rx gain** – Measure of how much amplification was applied to the signal received at the DSLAM port. **dn att est** – Measure of the downstream transmission loss on the DSL line. **up att est** – Measure of the upstream transmission loss on the DSL line.	

DSL Monitoring Interfaces Screens

Use the Interfaces screens to display read-only system information about interfaces.



▶ Procedure

To view the active interfaces list and interface status list:

1. Follow this menu selection sequence:

   Monitoring → *Interfaces* (**B-C**)

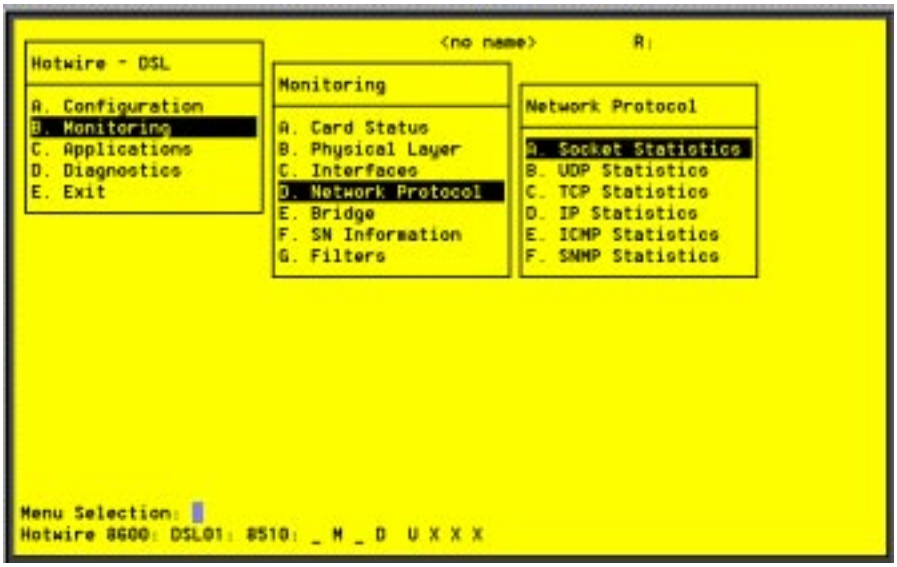
2. The Monitor Interfaces menu appears. Select the submenu option as shown in Table 5-3 and press Enter.

Table 5-3. Monitor Interfaces Options

Active List (Active Interfaces List)	**B-C-A**
Displays a list of the current status of all of the active interfaces in the card. **if** – Number of the interface. **name** – Name of the interface. **type** – Interface type (static). **link** – Name of the protocol on the interface. **state** – Current state of the interface. **ll-state** – Not applicable. **port** – Port linked to this interface. The only information that changes on this screen is the state (active or port-wait) column.	
Status (Interface Status)	**B-C-B**
Displays a list of additional information, after a specific interface (port) has been selected. **if name** – Enter the name of the desired interface. **protocol** – Type of protocol for the entered interface name. **port** – Port linked to this interface. **restarts** – Number of times interface has been restarted. **user** – <na> or none. **type** – Static. **link-downs** – Number of times the link has gone down. **state** – Active or prtwait. **inactivity T/O** – Number of times the interface has timed out.	

DSL Network Protocol Screens

Use the Network Protocol screens to display read-only system information for the management domain.



▶ Procedure

To view various management traffic statistics between the access node and the MCC card, including socket statistics, UDP statistics, TCP data and connection statistics, IP statistics, ICMP statistics, and SNMP statistics (these statistics only apply to traffic over the backplane):

1. Follow this menu selection sequence:

   Monitoring → *Network Protocol* (**B-D**)

2. The Network Protocol menu appears. Select the submenu option as shown in Table 5-4 and press Enter.

Table 5-4. Network Protocol Options (1 of 5)

Socket Statistics	**B-D-A**
Displays management domain information for the interface. Enter the socket name from the active socket list to view information on the application assigned to the specified socket number. **Start Socket** – Enter the socket number to start the active socket list. **Active Socket List** – This is the heading information for the following fields. It lists all the information about the currently selected socket. In addition, the lower right-hand corner of the screen displays a Socket Statistics window with detailed information about the selected destination. The Socket Statistics window displays the following information: **Socket** – Socket number. **Socket name** – Internal name of the socket. **Family** – Family of this socket (DARPA Internet). **Type** – Socket type (stream or datagram). **Local** – Port number on this card. **Remote** – Port number on remote card. **State** – Current state of the socket. **Input Bytes** – Bytes waiting in the socket for the owning application to process (will go to 0 when processed by the application). **Send Bytes** – Bytes waiting to be sent out to the remote machine. **PDU Drops** – Incoming packets dropped (usually due to a lack of space). **Byte Drops** – Outgoing packets dropped (usually due to a lack of space).	
UDP Statistics	**B-D-B**
Displays information on User Datagram Protocol (UDP) statistics for packets that terminate on the DSL card. The counters increment in real time and you may press Ctrl-r at any time to reset the counters. **Output Packets** – Number of UDP packets sent out of the card. **Input Packets** – Number of UDP packets coming into the card. **No Receive Port** – Number of UDP packets coming into the card that had no receive port waiting. **Unchecksummed** – Number of UDP packets coming into the card that had no checksum. **Header Error** – Number of UDP packets coming into card that had an error with the packet header. **Incorrect Checksum** – Number of UDP packets coming into the card that had a bad checksum. **Bad Length** – Number of UDP packets coming into the card that are an illegal length (too short). **Other Error** – Number of UDP packets coming into the card that had an error, but not one of the above.	

Table 5-4. Network Protocol Options (2 of 5)

TCP Statistics (TCP Data Statistics)	B-D-C

Displays a summary of the Transmission Control Protocol (TCP) data activity (packets and bytes transmitted and received) over the backplane of the MCC card. The TCP statistics is measuring packets that terminate on the DSL card.

The left column displays received data and the right column displays transmitted data. The counters increment in real time and you may press Ctrl-r at any time to reset the counters.

Left column:

Packets Received – Number of TCP packets received by the card.

acks – Number of acknowledgements received for transmitted packets. (Also shows the number of bytes that were acknowledged as received by the remote system.)

duplicate acks – Number of duplicate acknowledgements received.

acks for unsent data – Number of acknowledgements received for data that has not been sent yet.

pkts/bytes rcvd in-sequence – Number of packets/bytes correctly received in sequence for data that had to be split in multiple TCP packets.

dupl pkts/bytes – Number of duplicate packets/bytes received.

pkts/bytes w. some dup. data – Number of packets/bytes with some duplicated data. (Duplicated data is discarded by TCP.)

pkts rcvd out-of-order – Packets received out of order.

pkts of data after window – Packets of data received after receive window is full.

window probes – Packets received looking for space in the receive window.

window update pkts – Packets received from the remote system advertising a new window size.

pkts rcv after close – Packets received after the TCP connection is shut down.

discarded for bad checksum – Packets that were discarded because the checksum failed.

discarded for bad header offset fields – Packets discarded because the TCP header was corrupted.

discarded because packet too short – Packets discarded because the packet was too short (not a complete TCP header).

Right column:

Packets Sent – Number of TCP packets sent by the card.

data pkts – Number of the sent packets that were data packets instead of TCP control packets.

data pkts retransmit – Number of packets that had to be transmitted.

ack-only pkts – Number of sent packets that contained only an acknowledgement of a received packet and no additional data.

URG only pkts – Number of packets that contained only an Urgent flag and no data.

window probe pkts – Number of packets that were window probes.

window update pkts – Number of packets that were advertising new window size.

control pkts – Number of SYN, FIN, and RST control packets sent (Sync, Finish, and Reset flags).

Table 5-4. Network Protocol Options (3 of 5)

TCP Connection Statistics	B-D-C
When you press Return on the TCP Data Statistics screen, the TCP Connection Statistics screen is displayed, showing a summary of the TCP connection activity on all interfaces that terminate on the DSL card.	
connection requests – Number of TCP connections initiated by a process on this card.	
connection accepts – Number of TCP connections accepted by this card.	
connections established – Number of connections established.	
connections closed/dropped – Number of connections closed (normally) including those dropped.	
embryonic connections closed – Number of connections dropped before data transfer.	
segments updated rtt – Number of packets that updated the Round Trip Time (RTT) and the total number of times TCP attempted to update the RTT.	
retransmit timeouts – Number of times a packet had to be transmitted because it was not acknowledged and the number of times a connection was dropped because a packet could not be transmitted.	
persist timeout – Number of times the TCP persistence timer went off and sent a probe to the remote system.	
keepalive timeouts – Number of times a TCP keepalive request timed out.	
keepalive probes sent – Number of TCP keepalive probes sent.	
connections dropped by keepalive – Number of connections dropped because the keepalive timer failed to get any responses.	
IP Statistics	**B-D-D**
Displays a summary of the IP activity on all interfaces that terminate on the DSL card.	
total pkts rev – Total number of IP packets received by this card, with errors broken down on the right of the screen.	
fragments rev – Number of packet fragments received, with dropped fragments on the right of the screen.	
packets were fragmented on transmit – Number of packets that were fragmented on transmit.	
packets were received on transmit – Number of packets that were fragmented on transmit and the number of fragments that were created by those packets.	
packets forwarded – Number of packets that were forwarded to another system.	
packets not forwardable – Number of packets that could not be forwarded. (Usually due to packet errors or routing problems.)	
packet redirects sent – Number of redirect messages sent to other systems because they sent a packet that should not be sent to this card.	
network broadcasts received for local networks – Number of network broadcasts received for local networks.	
network broadcasts forwarded by media broadcast – Number of network broadcasts forwarded by media broadcast.	
network broadcasts partially processed – Number of network broadcasts dropped due to an error.	

Table 5-4. Network Protocol Options (4 of 5)

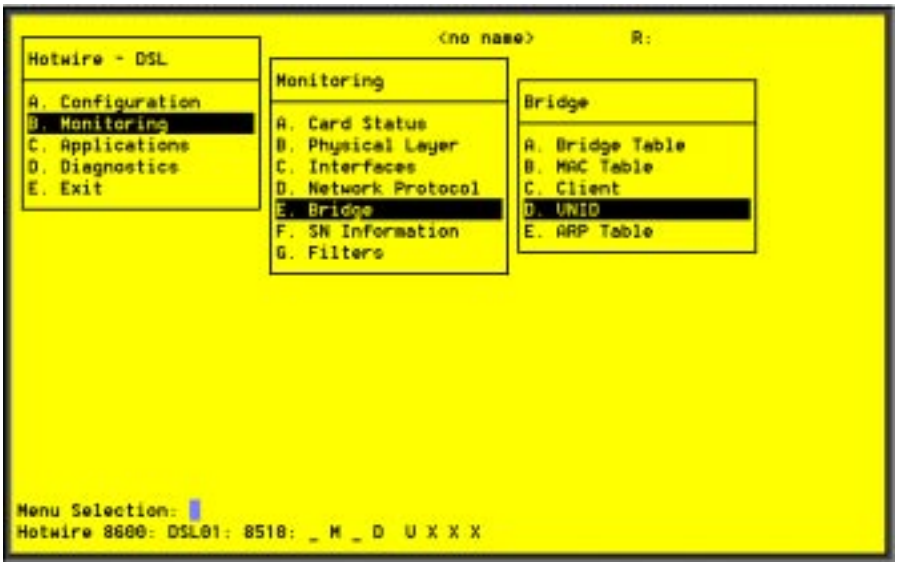
ICMP Statistics (ICMP Packet Statistics)	**B-D-E**
Displays a summary of the Internet Control Message Protocol (ICMP) activity on the backplane that terminates on the DSL card, such as echo replies. The columns show output and input packet counts. The counters increment in real time and you may press Ctrl-r at any time to reset the counters. Press Return to see more ICMP statistics.	
SNMP Statistics	**B-D-F**
Displays information on Simple Network Management Protocol (SNMP) statistics. The counters increment in real time and you may press Ctrl-r at any time to reset the counters. **In Packets** – Total number of SNMP PDUs received by the agent. **Get Requests** – Total number of SNMP Get Request PDUs accepted and processed by the SNMP agent. **Get Next Requests** – Total number of SNMP Get Next PDUs accepted and processed by the SNMP agent. **Total Requested Variables** – Total number of Management Information Base (MIB) retrieved successfully by the SNMP agent as a result of receiving valid SNMP Get Request and Get Next PDUs. **Set Requests** – Total number of SNMP Set Requests PDUs accepted and processed by the SNMP agent. **Total Set Variables** – Total number of MIB objects modified successfully by the SNMP agent as a result of receiving valid SNMP Set Requests PDUs. **ASN.1 Parse Errors** – Total number of Abstract Syntax Notation One (ASN.1) or Bit Error Rate (BER) errors encountered when decoding received SNMP messages. **Out Packets** – Total number of SNMP PDU responses sent by the agent. **Out Too Big Errors** – Total Number of SNMP PDUs generated by the SNMP agent for which the value of error status field is too big. **Out No Such Names** – Total number of SNMP PDUs generated by the SNMP agent for which the value of error status field is “no such name.” **Out Bad Values** – Total number of SNMP PDUs generated by the SNMP agent for which the value of the error status field is bad value. **Out General Errors** – Total number of SNMP PDUs generated by the SNMP agent for which the value of error status is Gen Err. **Read-only Errors** – Total number of SNMP PDUs delivered by the SNMP agent for which the value of the error status field is read-only. **Out Get Response** – Total number of Get-Response PDUs sent out by the SNMP agent. **Out Traps** – Total number of SNMP Traps PDUs generated by the SNMP agent. **SNMP Status** – Indicates the state of the SNMP Agent. The first byte = error code and the second byte = sub-routine code.	

Table 5-4. Network Protocol Options (5 of 5)

SNMP Authentication Statistics	B-D-F
When you press Return on the SNMP Statistics screen, the SNMP Authentication Statistics screen is displayed, giving you additional Community Administration information. **Community Administration** – Number of SNMP PDUs with community based authentication. ■ Bad Versions – Total number of SNMP messages delivered to the SNMP agent for an unsupported SNMP version. ■ Bad Community Name – Total number of SNMP messages delivered to the SNMP agent that used an SNMP community name not known to the entity. ■ Bad Community Use – Total number of SNMP messages delivered to the SNMP agent that represent an SNMP operation not allowed by the SNMP community named in the message.	

DSL Bridge Screens

Use the Bridge screens to display read-only system information.



▶ Procedure

To view bridge information:

1. Follow this menu selection sequence:

   Monitoring → *Bridge* (**B-E**)

2. The Bridge menu appears. Select the submenu option as shown in Table 5-5 and press Enter.

Table 5-5. Bridge Options (1 of 3)

Bridge Table	**B-E-A**
Displays information on various bridge functions.	
Item – Enter the item number you wish to display from 1–16.	
VNID – VNID number from 2–4094, in VNID tagged mode. Default = Null in VNID untagged mode.	
Mux Fwd – Enable = traffic forced upstream (Disable = blank).	
IP Filter – Enable/Disable.	
IP Scoping – Enable/Disable.	
Domain Name – Domain name of the card. There can be up to 12 VNID addresses at a time, with a maximum of 30 characters each.	

Table 5-5. Bridge Options (2 of 3)

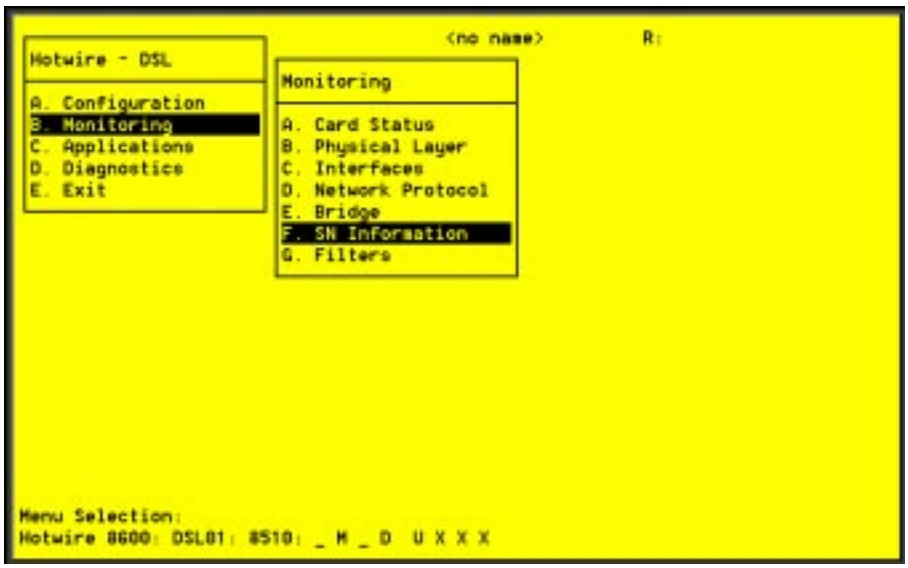
MAC Table	B-E-B
Displays the MAC table. **Bridge** – lb0 – Name of the Logical Bridge (Equivalent to e1a Ethernet). **Entry #** – Enter the MAC table entry number you wish to view. **Entries** – Number of entries in the MAC table. **Bridge Timer** – Timer that is used to show dynamic MAC addresses. # – Entry number. **MAC Address** – MAC address in *xx.xx.xx.xx.xx.xx* format. **VNID ID** – VNID ID associated with the MAC address. **Age (Secs)** – Age in seconds since the address was last used. **Intf** – Interface behind which the network element associated with the MAC address lies. **Flags** – Dynamic = MAC addresses that are determined via DHCP. Perm (DHCP) = MAC addresses are determined by the lease time. Entries in the MAC table will be removed when the lease time expires.	
Client	**B-E-C**
Displays information on specific clients or allowable subnets. **DSL Port #** – Enter the DSL port number 1–4 (Default = 1). **Item to Display** – Entry number. **Total** – Total number of users. **Item** – Enter the input number of the client (Default = 0). **IP Address** – Client IP address in *nnn.nnn.nnn.nnn* format (Default = 0). **Subnet Mask or Lease Expiration** – Variable based on Static or Dynamic entry. For static entries, Subnet Mask is used with IP address to specify a range of allowable static host IP entries to the Client table. For dynamic entries, Lease Expiration is the date and time when the client's DHCP lease expires. **NHR** – IP address of the default next hop router in *nnn.nnn.nnn.nnn* format. **VNID** – VNID between 2–4094 (Default = none). **Type** – S = Static or D = Dynamic. **Port Specific Parameters** – Enabled/Disabled. Shows active VNID information. NOTE: In order to display the following information, VNID has to be activated on the Port screen in the Configuration Bridge screen menu (**A-E-C**). Refer to Table 4-4, Bridge Options, in Chapter 4, *8310 MVL and 8510 RADSL Card Configuration.* **DNHR:** – Default next hop router name. **IP Scoping:** – Enabled/Disabled. **Mux Mode:** – Enabled/Disabled. **IP Filtering:** – Enabled/Disabled. IP source filtering.	

Table 5-5. Bridge Options (3 of 3)

VNID	**B-E-D**
Displays VNID information. **Item Number** – Enter the item to display. **VNID** – VNID between 2–4094 (Default = none). **Ports** – DSL ports that are members of the VNID. NOTE: The Ethernet interface is a member of all VNIDs.	
ARP Table	**B-E-E**
Displays the current Address Resolution Protocol (ARP) cache. **Line** – Sequential number of line. **IP Address** – Internet Protocol Address. **MAC Address** – MAC address associated with the IP address. (An incomplete can be shown in this column for some internal entries such as the backplane.) **Min** – Number of minutes since this entry was last used. **VNID** – VNID between 2–4094 (Default = none). **Flags** – Various flags associated with this entry. ■ PM = permanent ■ PB = publish this entry (respond for other hosts) ■ TR = trailers ■ PX = proxy ARP (card will proxy ARP for this IP address) ■ SB = subnet proxy ARP	

DSL SN Information Screen

Use the SN Information screen to display read-only Service Node information.



▶ Procedure

1. Follow this menu selection sequence:

   Monitoring → *SN Information* (**B-F**)

2. The SN menu appears. The information displayed on this screen is shown in Table 5-6.

Table 5-6. Service Node Options

SN Information	B-F
Displays Service Node information.	
Port # – Enter the DSL or MVL port number (1–4).	
SN Type – Model number of endpoint. For Model 8510, the SN is 5620. For Model 8310, the SN is 6310 MVL modem.	
System Name – 16 alphanumeric characters. Name assigned to the endpoint.	
System Contact – 32 alphanumeric characters. Name or number of the person responsible for the endpoint.	
System Location – 16 alphanumeric characters. Physical location of the system.	
Model Num – Model number of the endpoint.	
Serial Num – Serial number of the endpoint.	
Firmware Rev – Version of firmware.	
Hardware Rev – Version of hardware.	
CAP Rev – (For Model 8510 only) Version of CAP chipset.	
MVL Rev – (For Model 8310 only) Version of MVL chipset.	

DSL Monitoring IP Filters Screen

Use the IP Filters screen to display configured filters.

▶ Procedure

1. Follow this menu selection sequence:

   Monitoring → *Filters* → *IP Filters* (**B-G-A**)

2. The IP Filters screen appears. The information displayed on this screen is shown in Table 6-7.

Table 6-7. IP Filters

Filter Table	(B-G-A)
The Filter Table screen displays the status of the IP filter.	
Item # – Enter the item to display.	
Filter Name – Name of the IP filter.	
# of Rules – Number of rules in filter.	
Default filter action – Forward/discard.	
VNID – Interface and VNID to which the filter belongs.	
Port – Port to which the filter belongs: slc–s1f.	
Filter status – Active/Inactive.	
Direction – Inbound/Outbound.	
NOTE: To view the filter rules, you must have Administrator level access and use the Configuration Menu (**A-G-A**). Refer to Table 4-6, IP Filters Options, in Chapter 4, *8310 MVL and 8510 RADSL Card Configuration.*	

Diagnostics and Troubleshooting

6

Diagnostic Screens

Use the Diagnostics submenu to perform self-tests or view alarm status.

▶ Procedure

To view self-test, card alarm, packet test, and Service Node self-test information:

1. From the Hotwire – DSL Menu, select:

   Diagnostics (**D**)

2. The Diagnostics menu appears. Select the submenu option as shown in Table 6-1 and press Enter.

Table 6-1. Diagnostics Options

Selftest	**D-A**
Displays the results of the last disruptive self-test of the DSL card. This self-test is only performed on power up of the system or a reset of the card. Each subsystem (processors, memory, and interfaces) reports pass or fail. If all subsystems pass, the card has passed self-test. If a subsystem fails, reset or replace the card. You can determine when the self-test occurred by reading the elapsed time since the last reset on the card.	
Alarms (Card Alarms)	**D-B**
Displays all active card alarm conditions. Major alarms include Selftest Failure, Processor Failure (Sanity Timer), and DSL or Ethernet Port Failures. Refer to Table 6-2, Major Alarms. Minor alarms include Config Error (configuration has been corrupted) and Threshold Exceeded for DSL Margin or Link Down events. Refer to Table 6-3, Minor Alarms.	
DSL Packet Echo Test	**D-C**
Gives the user the ability to conduct a nondisruptive packet test between the DSL card and Hotwire Service Node endpoint. Test packets are sent to the Service Node at 10 percent of the line rate and echoed back to this card, where they are counted and checked for errors. The running time of the test can be specified and the test will continue until the specified time has elapsed or the test is stopped. Results include packets sent, valid packets received, errored packets received, errored seconds, and elapsed time of the test. NOTE: You can specify the DSL port number but only one port can be tested at a time.	
SN Selftest	**D-D**
Gives the user the ability to perform a power-on Service Node self-test. A port number can be selected to perform the test. NOTE: Entering yes in the Reset SN field will temporarily disrupt the data path on the specified DSL port while the SN resets.	

Troubleshooting

The status of each card in the Hotwire DSLAM is indicated on the Card Selection screen (see *Components of a Hotwire Screen* in Chapter 2, *Hotwire Menus and Screens).*

Checking Alarms

If the Card Selection screen indicates that a Major or Minor Alarm is on a card, follow the menu selection sequence *Diagnostics* → *Alarms* (**D**-**B**) to determine the cause of the alarm.

No Response at Startup

DSL cards do not respond at startup after rebooting chassis. Reset the MCC card. Be sure LEDs go through the reset sequence twice within about one minute.

If a DSL card does not appear on the Card Selection screen because the MCC card can no longer communicate with it, the MCC card will generate a major alarm. Follow the MCC's menu selection sequence *Monitor* → *Card Status* → *Syslog* (**B-A-C**) and view the event on the MCC Card System Log.

Major Alarms

Use Table 6-2 to determine the appropriate action to take for each Major Alarm.

Table 6-2. Major Alarms (1 of 2)

Alarm	Action
Selftest Failure	1. Check the Self-test Results display by following the menu selection sequence: *Diagnostics* → *Selftest* (**D**-**A**) 2. Do another Selftest (Reset) and check results. – If the results are normal, the problem was transient. Log the results. – If the results are the same as the first self-test, the card should be replaced. If only one port on a DSL card is bad, that port can be disabled. You may continue to use the card until it is convenient to replace it.
Processor Failure (Sanity Timer)	1. Check the Selftest Results display by following the menu selection sequence: *Diagnostics* → *Selftest* (**D**-**A**) 2. Do another Selftest (Reset) and check results. – If the results are normal, the problem was transient. Log the results. – If the results are the same as the first self-test, the card should be replaced.

Table 6-2. Major Alarms (2 of 2)

Alarm	Action
Ethernet Port Failure	1. Check cable connections to the DSLAM. – If cables are terminated properly, go to Step 2. – If cables are not terminated properly, terminate them correctly. 2. Check cable connections to the hub or Ethernet switch. – If cables are terminated properly, go to Step 3. – If cables are not terminated properly, terminate them correctly. 3. Check the Activity/Status LED at the Ethernet hub. – If Activity/Status LED does not indicate a problem, go to Step 4. – If Activity/Status LED indicates a problem, take appropriate action. 4. Disconnect the Ethernet cable and replace it with a working cable from a spare port on the hub. – If the replacement cable works, the original is bad and should be permanently replaced. – If the replacement cable does not work, reconnect the original cable and go to Step 5. 5. Move the DSL card and cable to another (spare) slot. – If this solves the problem, the connector or interface panel connections for the original slot are bad. Schedule maintenance for the chassis and try to use the spare slot temporarily. – If this does not solve the problem, the DSL card is probably bad and should be replaced.
DSL Port Failure	1. Check the Selftest Results display by following the menu selection sequence: *Diagnostics* → *Selftest* (**D**-**A**) 2. Do another Selftest (Reset) and check results. – If the results are normal, the problem was transient. Log the results. – If the results are the same as the first self-test, the card should be replaced. If only one port on a DSL card is bad, that port can be disabled. You may continue to use the card until it is convenient to replace it.
DSL Card Not Responding (LEDs on card are out or MCC is showing an alarm.)	1. Check to see if the lights are out on the DSL card. – Plug the card into an empty slot to see if it responds. If not, the card is bad and needs to be replaced. – If the card responds in a different slot, the slot connector may be bad. Call your service representative. 2. Check to see if the DSL LEDs are on. – If not, pull the card out and plug it in again. – Reset the card from the MCC or DSL Main Menu. – Go to the MCC Main Menu and clear NVRAM. – Replace the card.

Minor Alarms

Use Table 6-3 to determine the appropriate action to take for each Minor Alarm.

Table 6-3. Minor Alarms (1 of 2)

Alarm	Action
Config Error	1. Check the Selftest Results display by following the menu selection sequence: *Diagnostics* → *Selftest* (**D**-**A**) 2. Do another Selftest (Reset) and check results. – If the results are normal, the problem was transient. Log the results. – If the results still show configuration corruption, there is a card problem. The card's nonvolatile RAM should be erased and the configuration reentered. Perform a configuration download. – If the configuration has not been saved, use reset and erase NVRAM to force the card to the factory default. Enter the basic default route to the MCC and reconfigure the card manually.
NOTE: The following are minor alarms where thresholds have been exceeded and are primarily indications of degraded quality on the DSL loop. They are not necessarily related to problems with the DSL card.	
Margin Threshold (A trap message is sent if margin falls below selected value.)	■ If DSL speed is set to a Fixed Rate, you may choose to lower the speed in the direction indicated by the threshold alarm (Fixed Up Speed or Fixed Down Speed) to get a better Margin and improved error performance. ■ If DSL speed is set to Rate Adaptive and the Margin Threshold is greater than 0, this alarm is a warning that the loop has degraded. The actual bit rate should still be above 10^{-7}. This condition may be temporary due to high temperature or humidity/rain, or it may be permanent due to high noise from additional digital circuits installed in the same cable bundle. ■ If DSL speed is set to Rate Adaptive and the Margin Threshold is greater than 0, this alarm is a warning that the loop has seriously degraded. The actual bit rate may be below 10^{-7}. This condition may be temporary or permanent. However, if it persists, the loop may have to be reengineered for better performance by performing one of the following: – Remove bridge taps. – Change cable gauge on a cable section. – Run new cable. – Remove other noise-generating digital circuits from the cable bundle.

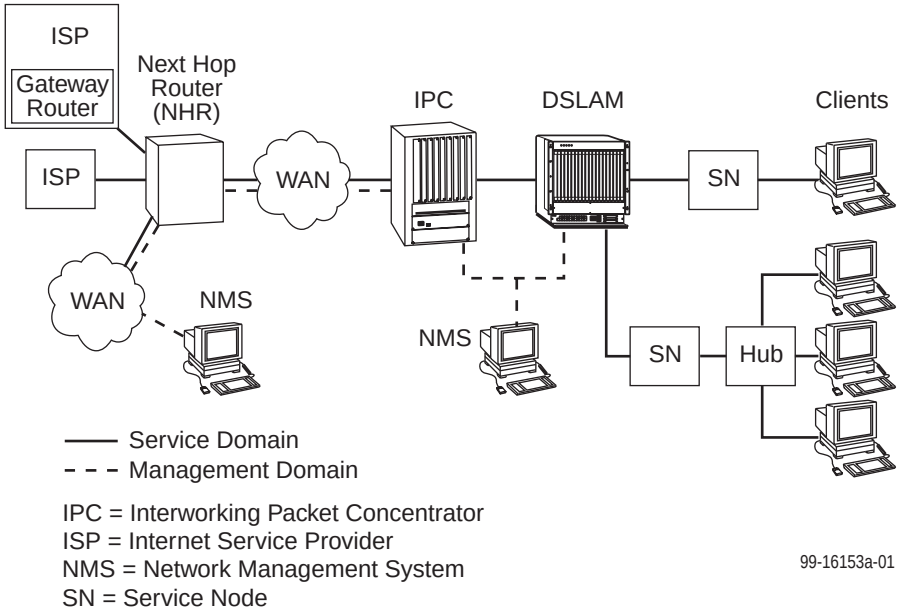
Table 6-3. Minor Alarms (2 of 2)

Alarm	Action
Link Down Threshold (A trap message is sent if the number of DSL link down events in 15 minutes exceeds the selected value.)	■ If the threshold is set low (1–4) and the link is currently down, then there may be a local loop or Service Node problem. Check both. – Verify that the Service Node is powered up, is connected to the local loop, and has passed its self-test. – Check the loop for continuity. ■ If the threshold is set low (1–4) and the link is currently up, then an event had occurred to temporarily knock out the connection. Log the event and continue normal operation. ■ If the threshold is set high (more than 4) and the link is currently down, then check the Margin statistics over the past hour and day. If the numbers are low, there may be a situation where the DSL modems cannot train. This condition may be temporary or permanent. However, if it persists, the loop may have to be reengineered for better performance by performing one of the following: – Remove bridge taps. – Change cable gauge on a cable section. – Run new cable. – Remove other noise-generating digital circuits from the cable bundle. ■ If the threshold is set high (more than 4) and the link is currently up, then there may be a loose connection in the loop plant, or the loop is barely usable. Check the Margin. If the Margin is normal, there may be a loose connection. If the Margin is low, try reducing the speed of the DSL port.

Network Problems

To provide a practical aid in the isolation and resolution of Layer 2 network difficulties, the guidelines in this section provide information on troubleshooting a generic network containing the devices found in most networks.

The illustration below shows the generic network addressed by this chapter.



These procedures assume that Asynchronous Transfer Mode (ATM) is used on the link between the IPC and the next hop router (NHR).

High-Level Troubleshooting

The following high-level procedures help you isolate problems to a particular segment of the network.

- For static clients, make sure the client can Ping its own IP address. This confirms the IP address was successfully accepted by the client computer.
- Make sure the client's default gateway is the same as the IP address for the Bridge Virtual Interface (BVI) on the appropriate ISP router.
- An Address Resolution Protocol (ARP) table may have invalid entries if a recent configuration change took place anywhere on the network and not enough time has passed for the entry to expire. Check the ARP tables on the client, DSLAM, and router.
- Make sure a default route is configured on the MCC card (screen **A-E-A**).

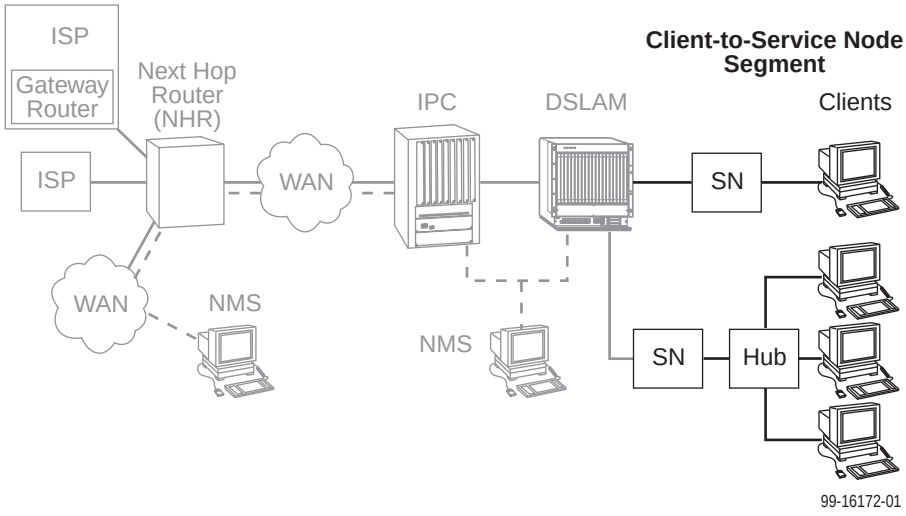
The following table provides an overview of the sequence of troubleshooting procedures for the DSL card. The following sections address potential problems that may occur in each network segment:

If the Client cannot Ping the Gateway Router and . . .	**Then . . .**
The Client cannot reach the SN	Refer to Table 6-4, Client-to-Service Node Segment.
The Client cannot reach the DSLAM	Refer to Table 6-5, Service Node-to-DSLAM Segment.
The Client cannot reach the IPC	Refer to Table 6-6, DSLAM-to-IPC Segment.
The Client cannot reach the Gateway Router	Refer to Table 6-7, IPC-to-Router Segment, and Table 6-8, Router-to-IPC Segment.

The tables in the following sections, each pertaining to a specific network segment, provide suggestions for resolving network problems.

Client Cannot Ping the Gateway Router

When the client cannot Ping the gateway router, specific fault-isolation procedures begin with the first network segment, client-to-service node (SN).



Client Cannot Reach Service Node

Table 6-4. Client-to-Service Node Segment

Layer	Solution
Layer 1 – Physical	1. Make sure the PWR LED on the front of the Service Node is lit. Use only the power adapter shipped with the unit. 2. To verify connection to the client, make sure the ETHERNET LED on the front of the Service Node is lit. 3. Make sure there is a physical connection between the Service Node and the Network Interface Card (NIC). If there is a LINK LED on the NIC card, make sure it is lit. 4. If there is a hub, check its cables and LEDs. 5. Make sure the correct type of cable is being used between the client and the Service Node. A crossover cable should be used if the client is not connected to a LAN hub. 6. Make sure the NIC and drivers are correctly installed. 7. Make sure the correct Service Node firmware is being used.
Layer 2 – Network	1. If static addressing is used, make sure the client has its correct IP address and subnet mask by entering the following: – Windows 95: **winipcfg** – Windows NT: **ipconfig/all** For other operating systems, use help or see the appropriate manual. 2. Restart the client after a static IP address has been added or changed. 3. Make sure the client can Ping its own IP address. This confirms the IP address was successfully accepted by the computer. 4. Check the PC's default gateway to make sure it is functioning properly.
	1. If dynamic addressing is being used and the client cannot get an IP address from the Dynamic Host Configuration Protocol (DHCP) server, statically configure an IP address and then verify that the client can Ping the DHCP server. 2. After the client reaches the server, remove the IP address and return the system to dynamic (DHCP) addressing.
	Make sure there are 32 or fewer DHCP users active on the port at any given time. Only 32 users are entered into the host table.

If the problem persists after the above items are checked, the client-to-service node segment of the network is functional.

Client Cannot Reach DSLAM

This section examines the Service Node-to-DSLAM segment of the network.

NOTE:

On the DSLAM, verify that the DSL link is up and that there is a MAC address for the client (screen **B-E-B**).

— If the MAC address appears, and all items in the previous section have been examined, it is safe to assume that this network segment is functioning. Skip this section and go to Table 6-6, DSLAM-to-IPC Segment.

— If a MAC address does not appear, check the items in Table 6-5.

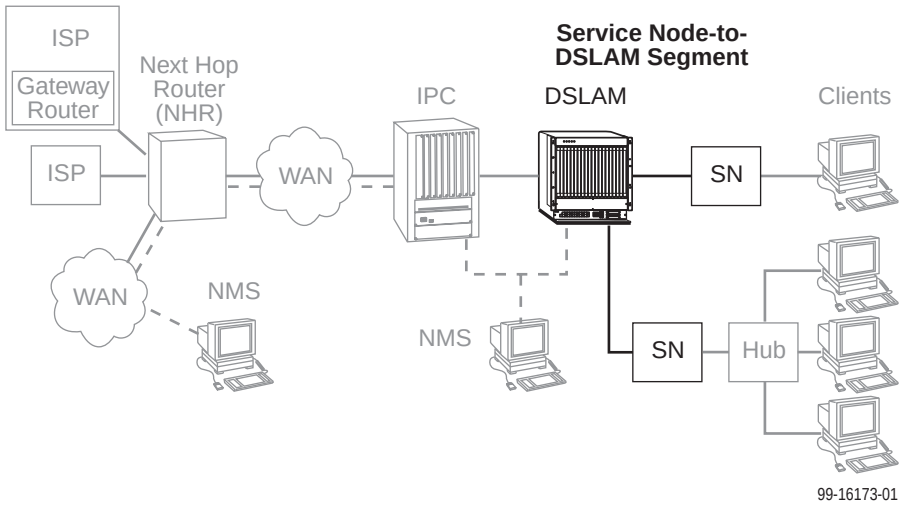


Table 6-5. Service Node-to-DSLAM Segment (1 of 2)

Layer	Solution
Layer 1 – Physical	1. On either the Service Node or Access Node, if the ALM LED is on, power the system off and then on again. Conduct a self-test from screen **D-A**. Go to screen **D-B** to learn more about the cause of the alarm. 2. Perform a Service Node self-test at the DSLAM (screen **D-D**) to test memory and start up parameters. 3. If the PWR, ALM, LINE and TST LEDs remain lit, make sure the correct power adapter is being used and that the correct firmware is on the Service Node (screen **B-F**). Make sure the correct port is selected. 4. Go to screen **B-A-C** to view the system log.

Table 6-5. Service Node-to-DSLAM Segment (2 of 2)

Layer	Solution
Layer 1 – Physical (continued)	5. Make sure the LINE LED on the Service Node is lit. This verifies a DSL connection to the DSLAM. 6. On the Access Node, make sure the LINE STATUS is up. 7. Make sure the CO splitter is connected correctly. The DSL line goes to the 50-pin amphenol jack on the DSLAM and the other line goes to the PSTN switch in the central office. 8. Make sure the 50-pin amphenol jack is firmly attached to the correct interface on the DSLAM. For the 20-slot chassis, the ports are labeled 1–6, 7–12, and 13–18. 9. Make sure the loop characteristics are within MVL/RADSL specifications.
Layer 2 – Network	1. On the DSLAM, if using static IP addressing, make sure the address is correctly configured (screen **A-E-D**). 2. On the DSLAM, make sure all configured ports are in use (screen **B-B-A**). If ports are not in use, properly configure them. 3. On the DSLAM, check the status of the port (screen **A-C-B**). If the status is not active, restart the port. 4. If dynamic addressing is being used and the clients cannot get an IP address from the DHCP server, statically configure an IP address and then verify that the client can Ping the DHCP server. After the client reaches the server, remove the IP address and return the system to dynamic (DHCP) addressing. 5. An ARP table may have invalid entries if a recent configuration change took place anywhere on the network and enough time has not passed for the entry to expire. Check the ARP tables on the client, DSLAM, and router. 6. To ensure connection between the DSLAM and the Service Node, perform a packet echo test (screen **D-C**). Make sure the number of packets sent is the same as the number of packets received. If fewer packets are being received than sent, the Service Node may not be functioning correctly. 7. If the DSLAM fails to connect to the Service Node, attempt to connect upstream and downstream at lower speeds or configure the card to rate adaptive mode (screen **A-B-B**). When a speed is changed, the port must be restarted (screen **A-C-B**) for the change to take effect.

If the problem persists after the above items are checked, the client-to-DSLAM segment of the network is functional.

Client Cannot Reach IPC

This section examines the DSLAM-to-IPC segment of the network.

NOTE:
On the IPC, verify that there is a MAC address for the client (enter the **macinfo** command). If the correct MAC address appears on the IPC, and all the items in the previous sections have been examined, it is safe to assume that this segment of the network is functioning properly. Skip this section and go to *Client Cannot Reach Router* on page 6-14. If a MAC address does not appear, check the items in Table 6-6.

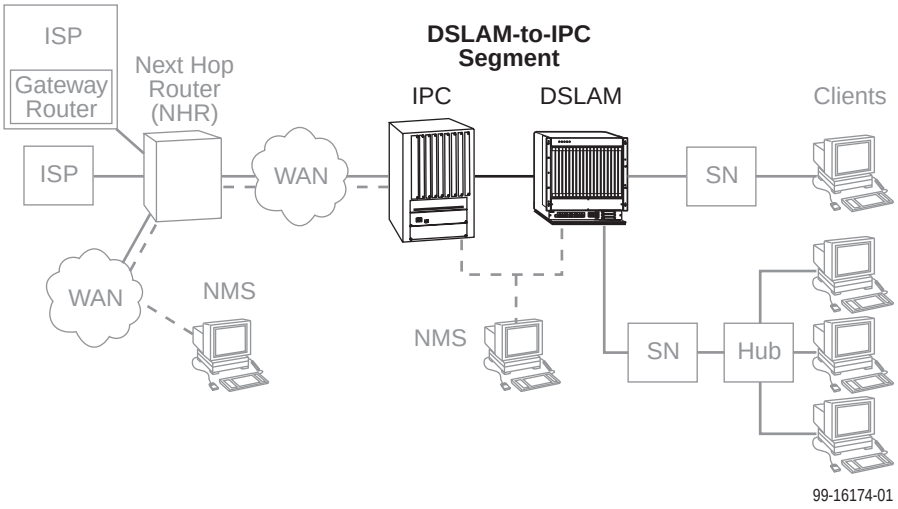


Table 6-6. DSLAM-to-IPC Segment

Layer	Solution
Layer 1 – Physical	If the DSL card shows an alarm, go to screen **D-B** to determine the cause. An Ethernet alarm usually means no connection to the IPC. Check the cable and make sure the correct type is being used.
	On DSLAM, make sure the Ethernet cable is plugged into the port number that corresponds to the slot number of the card.
Layer 2 – Network	If applicable, verify that the desired mode (tagged or untagged) is selected (screen **A-E-A**). Reset the card if a change is made.
	If tagged mode is enabled on the DSLAM: 1. Make sure a card VNID is configured (Card VNID screen). For each connection, the VNID number must be the same as the group number on the IPC. 2. Make sure a card VNID is entered (screen **A-E-B**). If tagged mode is disabled for VNID tagging, **`Card VNID`** should be **none**. NOTE: With firmware earlier than 3.2.3, follow Steps 3 and 4. For firmware later than 3.2.3, complete Step 4 only. 3. Make sure the appropriate VNID is active on the correct port (screen **A-E-C**). An asterisk (*) indicates the active VNID. If tagged mode is disabled, **none** should be active on each port. 4. Make sure the IPC Ethernet port is part of a 802.1q (VNID) group. To view VNID groups, enter **viqgp**.
	On the IPC: 1. For VLAN functionality, the mpm.cmd file must contain these lines: **`group_mobility=1`** **`move_from_def=1`** If necessary, add the lines and reboot the IPC. 2. Make sure that all modules are supported by their respective image (.img) files. Enter **ls** to view file names. 3. Enter **gp** to make sure the group is configured correctly.

Client Cannot Reach Router

Table 6-7 examines the IPC-to-Router segment of the network on the IPC end of the segment.

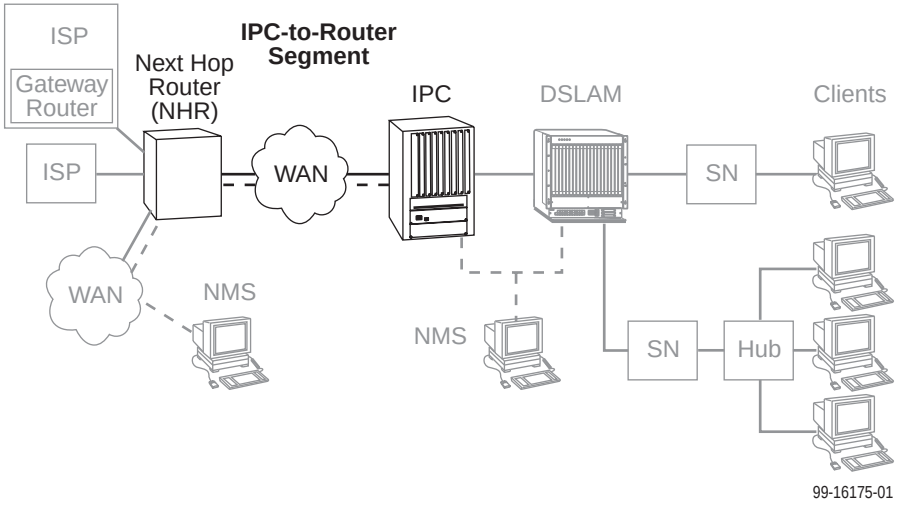


Table 6-7. IPC-to-Router Segment

Layer	Solution
Layer 1 – Physical	1. On the IPC, make sure the cables are firmly attached to the WAN interface. 2. If no CSU/DSUs are being used, either the router or the IPC must provide network clocking. Network clocking is usually provided by the device connected to the DCE cables. 3. If no CDU/DSUs exist between IPC and Router, make sure transmission lines are active by looking for appropriate LEDs. 4. If there is no connection between the router and IPC, invert the clocking on one or both DSU/CSUs.
Layer 2 – Network	On the IPC: 1. Set payload scramble to false. To turn PLScramble on or off on the IPC, type **map slot/port** (where slot/port is that of the ATM card) and set 10=1 to false. 2. If using SONET, make sure that the line characteristics are correct. Type **map slot/port** and select the Phy Media option. 3. Enter **vas** to make sure a service is configured. 4. Make sure encapsulation is the same as on the router (RFC1483). 5. Enter **vvc** to make sure vpi and vci are configured correctly. 6. Enter **vcs** to view ATM connection statistics. 7. Enter **vcrs** and **vcts** to view transmitted and received cells.

Table 6-8 examines the Router-to-IPC segment of the network from the router end of the segment.

Table 6-8. Router-to-IPC Segment

Layer	Solution
Layer 2 – Network	1. On the router, make sure that the defined line characteristics agree with the characteristics defined on the IPC. 2. Make sure a virtual circuit is configured under the respective ATM subinterface. The PVC number should correspond to the PVC number on the IPC. 3. Make sure a bridge-group number is configured under the respective ATM subinterface and that the BVI number is the same as the bridge-group number. 4. Make sure encapsulation on the router is the same as on the IPC (RFC1483). 5. Make sure the client's default gateway is the same as the IP address for BVI on the appropriate ISP router. 6. If a Ping from the client is not successful, issue a **show ARP-cache** command on the router to make sure the correct MAC address and client IP address appear.

Cannot Upload Configurations to a UNIX Server

▶ Procedure

If the TFTP server denies write permission and displays the message **`TFTP recv failure`**:

1. Before uploading configurations, create a dummy file and give it global Read-Write permissions.
2. Configure TFTP host to have Write permissions in the specified directory.

Performance Issues – Viewing Network Statistics

The previous sections of this document examined connectivity issues, i.e., the inability to Ping the router. Table 6-9 presents information on viewing DSLAM statistics screens to examine performance issues.

These statistic screens give information related to the number of packets transmitted and received on an interface as well as any packet failures. Refer to Table 5-2, Physical Layer Options, in *Monitoring the Hotwire DSLAM* of the *Hotwire Management Communications Controller (MCC) Card, IP Conservative, User's Guide* for details on the Statistics screens.

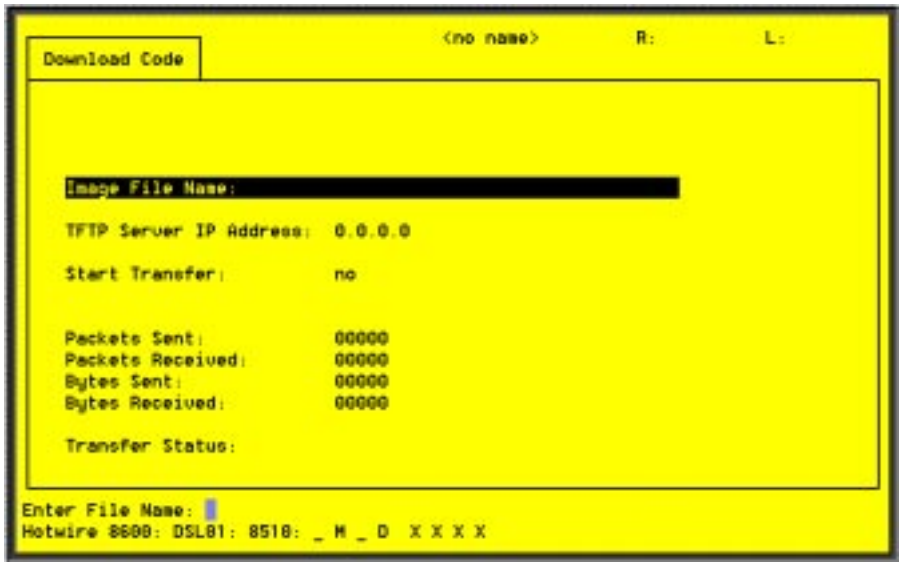
Table 6-9. Examining Performance Issues

To . . .	Go To . . .
View Statistics	■ Screen **B-B-B** to view Ethernet statistics. ■ Screen **B-B-C** to view HDLC statistics. ■ Screen **B-B-D** and choose a port to view the DSL Link performance summary. ■ Screen **B-B-E** and choose a port to view how many packets are on the link, view DSL performance statistics. ■ Screen **B-B-F** to view Error statistics and choose a port. ■ Screen **B-B-G** to view Transmit statistics and choose a port. ■ Screen **B-A-C** to view System Log.
Examine Slow Performance	Screen **B-B-B**. Slow performance could result from errors seen on this screen. Make sure the DSLAM and IPC are both operating at either full- or half-duplex mode. On the DSLAM, go to screen **A-B-A**. On the IPC, enter **10/100cfg**. If operating at full-duplex, a hub should not be used. Check the Ethernet Statistics screen for excessive Cycle Redundancy Check (CRC) errors, a bad connection, or a bad cable (see *DSL Monitoring Physical Layer Screens* in Chapter 5, *Monitoring the Hotwire DSLAM*).
Examine Collisions	Screen **B-B-B**. Minimal collisions are acceptable if packets are not being discarded. Excessive collisions could result from forcing too much data over a single Ethernet. 1. Determine if your network is too large or long (single Ethernet cable or end-to-end cable). 2. Check to see if there are too many repeaters. 3. Check to see if there are too many users on a single Ethernet. Intranetworking communication problems: 1. Verify that the internetworking network cables meet IEEE standards for local Ethernet networks. 2. Check cable connections to DSLAM and other devices in the network. 3. Determine whether or not your system is the only one in the network with a problem.

Download Code

A

The Download Code menu option on the Hotwire DSLAM gives you the ability to upgrade your software with a new version of code and then apply this code to your system.



New firmware releases are typically applied to the MCC card, DSL cards, and/or endpoints in your system.

When a software upgrade affects both the MCC and the DSL cards, you must download and apply a new version of code into each of the DSL cards **before** you download and apply a new version of code into the MCC.

When you are downloading code to an endpoint, configure your TFTP server with the following timeout values:

- **Retransmission timeout** – Value not less than 10 seconds.
- **Total transmission** – Value not less than three times the retransmission timeout.

You can also use the above values for a standard TFTP transfer.

Download Code

When you are attempting to download to the DSL cards, refer to Table 5-1, Card Status Options, in Chapter 5, *8310 MVL and 8510 RADSL Card Configuration*. In general, the following describes what to expect when you have initiated a download from the configuration menu.

From the DSL Configuration Main Menu, follow the menu selection sequence:

Configuration → *Card Status* → *Download Code* (**A-A-F**).

This brings you to the Download Code submenu. Select Download Code (**A**).

NOTE:

To download code to the Service Node(s), you must use the MCC download menu. For information on this and other methods used to download firmware to the DSL and MVL cards, see *Configuration Options* in the *Hotwire Management Communications Controller (MCC) Card, IP Conservative, User's Guide*.

Download Only System: Automatic Immediate Apply

Before initiating a download, go to the MCC card and verify that you can Ping the TFTP server. If you cannot, do not proceed with the download. Also, make certain that the files that you are going to download from exist in the system.

In order for the system to become fully functional again, you **must** start the Download Code file transfer procedure. Enter the image file name and the TFTP Service IP address. Select **Yes** to begin the file transfer. When the file transfer has successfully completed, the system will automatically restart and become fully functional with the newly acquired firmware.

Traps

B

DSL Card Traps

Traps are configured via a Telnet or terminal session. The addition or removal of a card or another hardware component within the Hotwire DSLAM system causes a trap to be generated. These traps indicate a configuration change notification (CCN) of a card (a hardware replacement or a software upgrade).

Event	Severity	Comment	Trap #	MIB
CCN (Configuration Change Notice)	warning	Configuration change caused by one the following events: ■ Software download. ■ Configuration download. ■ Card removed (objective).	7	hot_sys.mib (Enterprise MIB)
	warning	Configuration change affecting the entity MIB.	1	hot_domain.mib (Enterprise MIB)
Cold start	warning	Card has been reset and performed a cold start.	0	MIB II (RFC 1213)
Configuration download failure	warning	Configuration download has failed.	2	hot_diag.mib (Enterprise MIB)
Device failure	major	Access Node's software has detected an internal device failure.	15	hot_sys.mib (Enterprise MIB)
DHCP filter security failure	minor	Cannot add new route; route table contains maximum number of rules.	11	hot_dhcp.mib (Enterprise MIB)
xDSL link up or down *or* Transitions threshold exceeded	minor	Number of link down events above threshold. This rate is limited to once every 15 minutes.	1	hot_xdsl.mib (Enterprise MIB)
xDSL margin low	minor	Margin estimate below customer set threshold.	3	hot_xdsl.mib (Enterprise MIB)

Event	Severity	Comment	Trap #	MIB
xDSL margin normal	normal	Margin estimate now above customer set threshold.	103	hot_xdsl.mib (Enterprise MIB)
xDSL port failure	major	Processor detected bad DSL modem chip set.	5	hot_xdsl.mib (Enterprise MIB)
xDSL port operational	normal	Processor now communicating with DSL modem.	105	hot_xdsl.mib (Enterprise MIB)
xDSL port speed low	warning	Port speeds decreased to lower bound thresholds.	2	hot_xdsl.mib (Enterprise MIB)
xDSL port speed normal	normal	Port speed now above lower bound threshold.	102	hot_xdsl.mib (Enterprise MIB)
xDSL port speed normal	normal	Port speed now above lower bound threshold.	102	hot_xdsl.mib (Enterprise MIB)
xDSL SN selftest fail	warning	Self-test failure from an Service Node.	19	hot_xdsl.mib (Enterprise MIB)
xDSL test start	normal	Test started by any means.	6	hot_xdsl.mib (Enterprise MIB)
xDSL test clear	normal	Test over.	106	hot_xdsl.mib (Enterprise MIB)
Dynamic filter injection failure	warning	Cannot inject or delete dynamic filters to Service Node on port *n.*	10	hot_dhcp.mib (Enterprise MIB)
Ethernet link down	major	—	2	MIB II (RFC 1213)
Ethernet link up	normal	—	3	MIB II (RFC 1213)
Warm start	warning	Power on reset.	1	MIB II (RFC 1213)
Self-test failure	minor	Sent if any portion of the Access Node's restart/self-test fails.	16	hot_sys.mib (Enterprise MIB)
SN device failure	major	Operating software has detected an internal device failure but the Service Node is operating.	18	hot_xdsl.mib (Enterprise MIB)
SN device mismatch	minor	Service Node identified on port *n* does not match device described in port configuration role.	07	hot_xdsl.mib (Enterprise MIB)
SN device mismatch clear	minor	Service Node on port *n* now matches port configuration table.	107	hot_xdsl.mib (Enterprise MIB)
SN fatal reset	—	Variable binding field contains device failure code.	20	hot_xdsl.mib (Enterprise MIB)

Event	Severity	Comment	Trap #	MIB
SN loss of power	minor	Card received “last gasp” message from Service Node, followed by a link down condition one minute later.	17	hot_xdsl.mib (Enterprise MIB)
SN self-test failure	minor	Failure of the Service Node’s hardware components. This trap is only sent if the hardware failure still allows sending traps.	19	hot_xdsl.mib (Enterprise MIB)

Glossary

10BaseT A 10-Mbps Ethernet LAN that works on twisted-pair wiring.

address A symbol (usually numeric) that identifies the interface attached to a network.

agent (SNMP) A software program housed within a device to provide SNMP functionality. Each agent stores management information and responds to the manager's request for this information.

AN Access Node. Also known as DSLAM.

ARP Address Resolution Protocol. Part of the TCP/IP suite, ARP dynamically links an IP address with a physical hardware address.

ASCII American Standard Code for Information Interchange. The standard for data transmission over telephone lines. A 7-bit code establishes compatibility between data services. The ASCII code consists of 32 control characters (nondisplayed) and 96 displayed characters.

ATM Asynchronous Transfer Mode. A high-speed, low-delay, connection-oriented switching and multiplexing technique using 53-byte cells to transmit different types of data simultaneously.

authentication server An authentication server can either be a RADIUS server or an XTACACS server and can be used to confirm an end-user system's access location.

backplane A common bus at the rear of a nest or chassis that provides communications and power to circuit card slots.

bandwidth The range of frequencies that can be passed by a transmission medium, or the range of electrical frequencies a device is capable of handling.

BER Bit Error Rate. The number of bits in error over a given period compared to the number of bits transmitted successfully.

BootP Bootstrap Protocol. Described in RFCs 951 and 1084, it is used for booting diskless nodes.

bps Bits per second. Bits per second. Indicates the speed at which bits are transmitted across a data connection.

broadcast A method of transmission. The simultaneous transmission to two or more communicating devices.

BVI Bridge Virtual Interface on a Cisco router.

byte A sequence of successive bits (usually eight) handled as a unit in data transmission.

CAP Carrierless Amplitude Modulation and Phase Modulation. A transmission technology for implementing a Digital Subscriber Line (DSL). The transmit and receive signals are modulated into two wide-frequency bands using passband modulation techniques.

central office CO. The PSTN facility that houses one or more switches serving local telephone subscribers.

client A device that receives a specific service, such as database management, from a server.

community name An identification used by an SNMP manager to grant an SNMP server access rights to MIB.

CPU Central Processing Unit. The main or only computing device in a data processing system.

CRC Cyclic Redundancy Check. A mathematical method of confirming the integrity of received digital data.

default route The address used for routing packets whose destination is not in the routing table. In Routing Information Protocol (RIP), this is IP address 0.0.0.0.

DHCP Dynamic Host Configuration Protocol. A Microsoft protocol for dynamically allocating IP addresses.

DHCP Relay Agent A system that detects and forwards DHCP discover or request messages to the appropriate DHCP server.

DHCP Server A server which uses DHCP to allocate network addresses and deliver configuration parameters to dynamically configured hosts.

domain A named group of machines on a network. In IP, a domain consists of a block of IP addresses with similar prefixes.

downstream In the direction of the customer premises.

DSL Digital Subscriber Line. DSL is a copper loop transmission technology enabling high-speed access in the local loop.

DSL card Digital Subscriber Line Card. The primary card in the Hotwire DSLAM system. It has one Ethernet port and four DSL ports.

DSLAM Digital Subscriber Line Access Multiplexer. DSLAM provides simultaneous high-speed digital data access and analog POTS over the same twisted-pair telephone line.

DSU/CSU Data Service Unit/Channel Service Unit. A device that combines the functions of a DSU and a CSU. It connects Data Terminal Equipment to the digital network, protects the line from damage, and regenerates the signal.

e1a Name of the DSL card's and MCC card's 10BaseT (Ethernet) interface.

Enterprise MIB MIB objects unique to a specific company's devices.

Ethernet A type of network that supports high-speed communication among systems. It is a widely-implemented standard for LANs. All hosts are connected to a coaxial cable where they contend for network access using a Carrier Sense, Multiple Access with Collision Detection (CSMA/CD) paradigm.

Ethernet address A six-part hexadecimal number in which a colon separates each part (for example, 8:0:20:1:2f:0). This number identifies the Ethernet communications board installed in a PC and is used to identify the PC as a member of the network.

filter A rule or set of rules applied to a specific interface to indicate whether a packet can be forwarded or discarded.

firmware Software that has been temporarily or permanently loaded into read-only memory.

FTP File Transfer Protocol. A TCP/IP standard protocol that allows a user on one host to access and transfer files to and from another host over a network, provided that the client supplies a login identifier and password to the server.

full-duplex The capability to transmit in two directions simultaneously.

gateway address The subnet that the end-user system is on.

half-duplex The capability to transmit in two directions, but not simultaneously.

HDLC High-Level Data Link Control. A communications protocol defined by the International Standards Organization (ISO).

host	A computer attached to a network that shares its information and devices with the rest of the network.
host routes	An IP address having a subnet mask of 255.255.255.255.
hub	A device connecting several computers to a LAN.
ICMP	Internet Control Message Protocol. An Internet protocol that allows for the generation of error messages, test packets, and information messages related to IP.
IEEE	Institute of Electrical and Electronic Engineers.
Internet	The worldwide internetwork that predominantly uses the TCP/IP protocol.
intranet	A private network or internet using Internet standards and software, but protected from public access.
IP	Internet Protocol. An open networking protocol used for internet packet delivery.
IP Address	Internet Protocol Address. The address assigned to an Internet host.
ISP	Internet Service Provider. A vendor who provides direct access to the Internet.
LAN	Local Area Network. A privately owned and administered data communications network limited to a small geographic area.
lb0	Logical Bridge. Equivalent to e1a.
link	The physical connection between one location and another used for data transmission.
MAC	Media Access Control. The lower of the two sublayers of the data link layer, the MAC sublayer controls access to shared media.
MAC Address	Media Access Control Address. The unique fixed address of a piece of hardware, normally set at the time of manufacture, and used in LAN protocols.
margin (DSL)	The additional noise, measured in dB, that would need to be added to the existing noise on a given DSL loop to bring the Bit Error Rate to IE–7 (10^7).
MCC Card	Management Communications Controller Card. The DSLAM circuit card used to configure and monitor the DSLAM.
MIB	Management Information Base. A database of managed objects used by SNMP to provide network management information and device control.
MTU	Maximum Transmission Unit.
MVL	Multiple Virtual Lines. A proprietary local loop access technology that permits several services to concurrently and discretely use a single copper wire loop.
MVL card	A card with MVL ports used in the 8600, 8800, or 8810 DSLAM.
MVL modem	An endpoint (customer premises) modem that provides high-speed Internet or corporate LAN access over twisted-pair copper lines using MVL technology.
NAP	Network Access Provider. The provider of the physical network that permits connection of service subscribers to NSPs.
NHR	Next Hop Router. The next router IP address to any given destination.
NMS	Network Management System. A computer system used for monitoring and controlling network devices.
NSP	Network Service Provider. A local telephone company or ISP that provides network services to subscribers.

NTP	Network Time Protocol.
NVRAM	Non-Volatile RAM.
OpenLane DCE Manager	A proprietary network management program used with HP OpenView that helps a network administrator manage SNMP devices.
packet	A group of control and data characters that are switched as a unit within a communications network.
PDU	Protocol Data Unit. A message containing protocol-specific information.
PING	Packet InterNet Groper. Used for testing and debugging networks, PING sends an echo packet to the specified host, waits for a response, then reports the results of its operation. Used as a verb, to PING means to use the program to verify the accessibility of a device. The PING program is supported from both the DSL and MCC cards.
POTS	Plain Old Telephone Service. Standard telephone service over the PSTN with an analog bandwidth of less than 4 Hz.
POTS Splitter	A device that filters out the DSL signal and allows the POTS frequencies to pass through.
PPP	Point-to-Point Protocol. as specified by Internet RFC 1661.
proxy ARP	Proxy Address Resolution Protocol (ARP). A technique for using a single IP address for multiple networks. A device responds to ARP requests with its own physical address, then routes packets to the proper recipients.
PSTN	Public Switched Telephone Network. A network shared among many users who can use telephones to establish connections between two points. Also know as dial network.
RADSL	Rate Adaptive Digital Subscriber Line. A technique for the use of an existing twisted-pair line that permits simultaneous POTS and high-speed data communication at adaptive symmetric and asymmetric rates.
rate adaption	The ability to automatically adapt when the port speed is lower than the line speed.
Router	A device that connects LANs by dynamically routing data according to destination and available routes.
Routing Table	A table used by a node to route traffic to another node in the multiplexer network.
RTT	Round Trip Time.
RTU	Remote Termination Unit. A DSL device installed at the customer premises.
s1c	Interface name of a DSL card's DSL port #1.
s1d	Interface name of a DSL card's DSL port #2.
s1e	Interface name of a DSL card's DSL port #3.
s1f	Interface name of a DSL card's DSL port #4.
Service Node	SN. Endpoint modem at the customer premise, also known as a Remote Termination Unit (RTU). There are two model types. See RADSL and MVL.
SNMP	Simple Network Management Protocol. Protocol for open networking management.
SNMP agent	An application level program that facilitates communication between an SNMP management system and a device. See NMS.
SNMP trap	A message sent to an SNMP manager to notify it of an event, such as a device being reset.

static route A user-specified permanent entry into the routing table that takes precedence over routes chosen by dynamic routing protocols.

subnet address The subnet portion of an IP address. In a subnetted network, the host portion of an IP address is split into a subnet portion and a host portion using an address (subnet) mask. This allows a site to use a single IP network address for multiple physical networks.

subnet mask A number that identifies the subnet portion of a network address. The subnet mask is a 32-bit Internet address written in dotted-decimal notation with all the 1s in the network and subnet portions of the address.

TCP Transmission Control Protocol. An Internet standard transport layer protocol defined in STD 7, RFC 793. It is connection-oriented and stream-oriented.

Telnet Virtual terminal protocol in the Internet suite of protocols. Allows the user of one host computer to log into a remote host computer and interact as a normal terminal user for that host.

terminal emulation Software that allows a PC to mimic the signals of a specific type of terminal, such as a VT100 or 3270, to communicate with a device requiring that terminal interface.

TFTP Trivial File Transfer Protocol. A standard TCP/IP protocol that allows simple file transfer to and from a remote system without directory or file listing. TFTP is used when FTP is not available.

TraceRoute A program that lists the hosts in the path to a specified destination.

trap (SNMP) A notification message to the SNMP manager when an unusual event occurs on a network device, such as a reinitialization.

UDP User Datagram Protocol. A TCP/IP protocol describing how messages reach application programs within a destination computer.

unicasting In ATM, the sending of a Protocol Data Unit (PDU) to a single destination.

upstream In the direction of the telephone network.

XTACACS See Authentication Server.

VNID Virtual Network ID.

WAN Wide Area Network. A network that spans a large geographic area.

Index

N

O

P

R

S

T